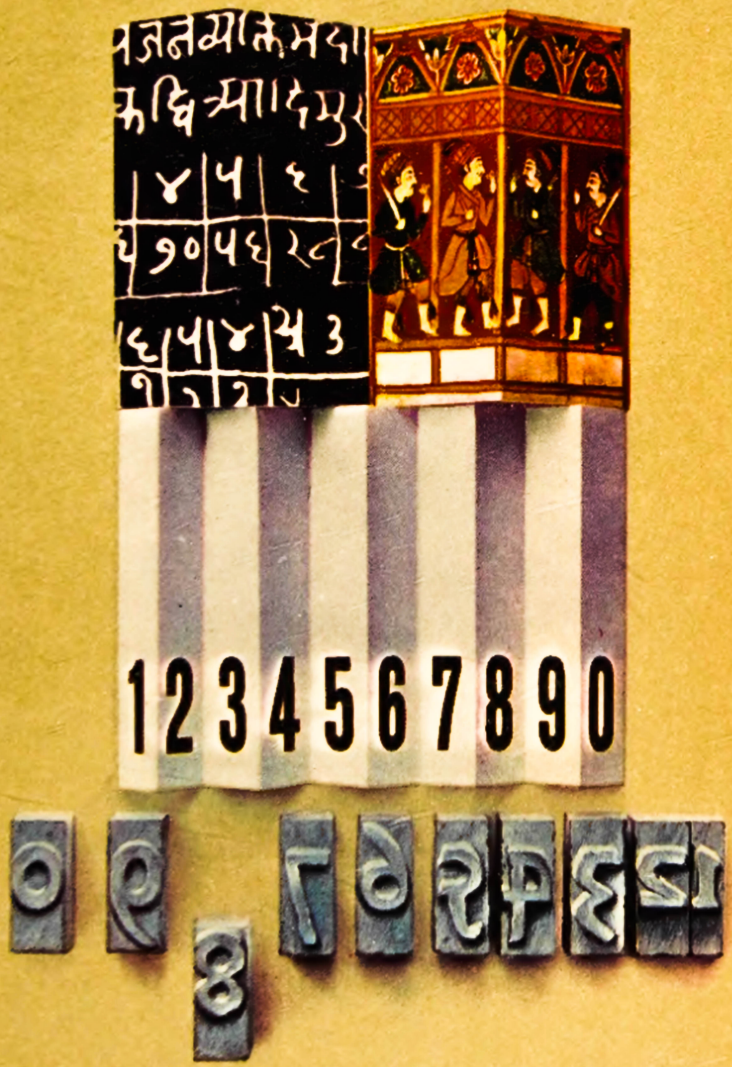
B. A. Venkov

Elementary number theory



The book now a classical, is a good general introduction of the theory of numbers with emphasis on aspects which are not so well treated elsewhere. The work has not so far received full attentions in the West. The points of special interest are:

- Gauss's treatment of cubic congruences
- The reproduction of Gauss's first proof of the quadratic reciprocity law
- The chapter on Liouville's method for dealing with representability by quadratic forms
- The exposition of Ouspensky's elementary treatment of the Kronecker class-number relations

ELEMENTARY NUMBER THEORY

B. A. VENKOV
University of Leningrad USSR

Elementary number theory

Translated from the Russian and edited by

HELEN ALDERSON
Cambridge University, Department of Pure Mathematics, England

WOLTERS-NOORDHOFF PUBLISHING GRONINGEN 1970
THE NETHERLANDS

© 1970 Wolters-Noordhoff Publishing Groningen, The Netherlands.

No part of this book may be reproduced in any form, by print, photoprint, microfilm or any other means without written permission from the publisher.

Library of Congress Catalogue Card Number 71-90854.

ISBN 90.01.89620.0

PRINTED IN THE NETHERLANDS BY
NV BOEKDRUKKERIJ DIJKSTRA NIEMEYER - GRONINGEN

FOREWORD

The present monograph's title 'Elementary number theory' does not completely describe its principal aim. For it collects together those results of the classical theory of numbers, and also those new discoveries, which can be achieved by purely arithmetical methods (i.e. without introducing the concepts of analysis, geometry, and irrational and complex numbers). Most of this material is generally 'Elementary' in the ordinary sense of the word. Irrational numbers occur only where they are essential (chapter II and some sections of chapter IV). This approach has been taken because algebraic, geometrical and analytical methods in the theory of numbers form the subject matter for other monographs in the present series.

TRANSLATOR'S ACKNOWLEDGEMENTS

The text of the book has been left completely original, although I have added footnotes in order to relate the text to the present-day advances in Number Theory. I should like to thank Professors L. J. Mordell, J. W. S. Cassels, A. Schinzel and J. Brillhart, and Dr. J. C. P. Miller, for their help and suggestions.

I am also grateful to Professors Mordell and Schinzel and numerous younger members of the Mathematics Department of Cambridge University, for their help in checking the proofs of the text.

This work was completed while the translator held a Calouste Glubenkian Research Fellowship at Lucy Cavendish College, Cambridge.

Helen Alderson (Popova)
Department of Pure Mathematics,
16, Mill Lane, Cambridge

TABLE OF CONTENTS

1. Basic concepts of the theory of numbers 1

1. The factorisation of a number into prime factors; Euclidean algorithm 1
2. Elementary arithmetical functions 2
3. Theorems on the divisibility of factorials 4
4. Theorems of Euler and Fermat; linear congruences 5
5. Theorems of Lagrange and Wilson 7
6. Primitive roots, indices, binary congruences 9
7. Bernoulli numbers 12
8. Quadratic residues; Gauss's third proof of the quadratic reciprocity law 14
9. The quadratic character to a composite modulus 18
10. Generalisations of congruences 20

Notes to Chapter 1 24

2. Continued fractions and the diophantine approximations 32

1. Farey series 32
2. The Dirichlet's principle. Theorems of Kronecker and Minkowski 34
3. Hermite's theorem 37
4. Continued fractions, the properties of convergents 39
5. The Legendre criterion; the theorems of Vahlen and Borel 42
6. Equivalent numbers 44
7. Relative minima of the form $x-\omega y$ 47
8. Arithmetical applications of Dirichlet inequality 48
9. Symmetric continued fractions 56
10. Development of a quadratic irrationality into a continued fraction 58
11. Inverse numbers 61
12. Pellian equation 62

13. The Johann Bernoulli problem 65
Notes to chapter 2 68

3. Power residues 72

1. Gauss's first proof of the quadratic reciprocity law 72
2. Distribution of power residues in a progression 75
3. Biquadratic residues; criteria for a number to belong to a biquadratic distribution class 82
4. Cubic residues; Gauss's method 89
5. Theorem on the residue of a in the decomposition $p = a^2 + 4b^2$ 93

Notes to chapter 3 95

4. Gauss's theory of quadratic forms 99

1. On representation of an integer by a binary quadratic form 99
2. Transformation of a form into itself 101
3. Reduction of forms of a negative determinant 104
4. Forms of a positive determinant 106
5. Periods of integral forms 111
6. Forms of a square determinant 115
7. Solution of a general quadratic equation in two unknowns 116
8. Order of forms. Representation of numbers by a complete system of non-equivalent forms of a given order 118
9. Ambiguous forms and classes. A special study of the periods 121
10. The composition of binary forms 127
11. Comparison of numbers of classes whose determinants differ by a square 134
12. Distribution of binary forms into genera 140
13. Ternary forms, finiteness of the number of classes, basic problems of the theory 146
14. Representation of numbers and binary forms by ternary forms 153
15. Application of Redei theorem to binary forms 161
16. Representation of numbers and of binary forms as a sum of three squares 164

Notes to chapter 4 171

5. Partitions. Liouville's methods 176

1. Point graphs, the Euler-Legendre theorem 176

2. Double partitions. Recurrence relations for additive functions 183
3. The Ramanujan theorem 187
4. Liouville's methods; deduction of fundamental identities 190
5. Representation of a number by a form in two, three and four variables 197
6. The number of representations of a number as a sum of 2, 4, 6, 8 and 10 squares 204
Notes to chapter 5 212

6. The class number of binary quadratic forms 215

1. Tables of class numbers. Regular determinants 215
2. The Kronecker relation between the numbers of classes 218
3. The Dirichlet formulae 227
4. Proof of the Dirichlet formulae for a properly primitive case of a negative determinant 230
Notes to chapter 6 238

Bibliography 243

Index 247

1. BASIC CONCEPTS OF THE THEORY OF NUMBERS

The present chapter presents a brief survey of the basic concepts in classical number theory.

§ 1. The factorisation of a number into prime factors; Euclidean algorithm

If two given integers a and $b \neq 0$ are such that the ratio a/b is an integer, then we say that a is *divisible* by b, or that a is a *multiple* of b, or that b is a *divisor* of a. An integer $p > 1$ is a *prime* if it has no other divisors apart from obvious ones ± 1, $\pm p$. The composition of all integers from primes is shown in the following fundamental theorem:

THEOREM 1. *Every integer* > 1 *can be represented uniquely as a product of prime factors, some of which may be equal to one another.*

The symbol $d = (a, b)$, $(d > 0)$ denotes the greatest common divisor of two integers a and $b \neq 0$. It can be found by means of the Euclidean Algorithm, namely, by performing successive divisions and obtaining the following sequence of equalities:

$$a = qb + r, \qquad b = q_1 r + r_1$$
$$r = q_2 r_1 + r_2, \ \ldots, \ r_{n-2} = q_n r_{n-1} + r_n, \quad r_{n-1} = q_{n+1} r_n, \tag{1}$$

in which $q, q_1, \ldots, r, r_1, \ldots$ are integers satisfying

$$0 < r < |b|, \quad 0 < r_1 < r, \quad 0 < r_2 < r_1, \ \ldots, \ 0 < r_n < r_{n-1}.$$

Equalities (1) present nothing else but the development of a number a/b into a simple continued fraction:

$$\frac{a}{b} = q + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \ddots + \cfrac{1}{q_{n+1}}}}. \tag{2}$$

From them we deduce: 1) that r_n divides a and b, 2) that every common divisor of a and b divides r_n. Consequently, $r_n = d$; eliminating from (1) $r_{n-1}, \ldots, r_1$ and r and using the properties of continued fractions, we obtain $d = Qa - Pb$, where $\pm P$ and $\pm Q$ are the numerator and the denominator of the last but one convergent to fraction (2). Thus we arrive at the classical solution of equation $aX - bY = d$ in integers X, Y by means of continued fractions.

When $d = 1$, integers a, b are called *relatively prime.* In this case it is evident from equation $Qa - Pb = 1$ that if ac is divisible by b, then integer c must be divisible by b, which yields theorem 1.

From the established properties of (a, b) similar properties may be deduced for the greatest common divisor $(a, b, \ldots, c)$ of several numbers $a, b, \ldots, c$ not simultaneously zero. Namely, $(a, b, \ldots, c)$ is equal to the greatest common divisor of a and $(b, \ldots, c)$ and may be represented as a linear form in $a, b, \ldots, c$ with integral coefficients. Similarly, the least common multiple of integers $a, b, \ldots, c$, not equal to zero, (i.e. the smallest non-zero integer which is divisible by every integer $a, b, \ldots, c$), is equal to the least common multiple of a and the least common multiple of $b, \ldots, c$. For two integers a, b the least common multiple is equal to $|ab|/(a, b)$.

Concerning the distribution of primes 2, 3, 5, 7, ... in the sequence of natural numbers no precise laws are known. We need point out only the important proposition already proven in 'Elements' by Euclid (book IX, 20) (see A. A. Vassiliev [85], pp. 27–44);

THEOREM 2. *The number of primes is infinite.*

In fact, if there is a definite number of primes $p_1, p_2, \ldots, p_k$ then to it can always be adjoined a new prime. Namely, every prime divisor of $p_1 p_2 \ldots p_k + 1$ is such a number.

§ 2. Elementary arithmetical functions

Let $n > 0$ be an integer. Considering all positive devisors of n, denote their number by $\tau(n)$ and their sum by $\zeta(n)$. Assuming, by theorem 1 $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$ where $p_1, p_2, \ldots, p_k$ are distinct primes and $\alpha_1, \alpha_2, \ldots, \alpha_k$ are positive exponents we find

$$\tau(n) = (\alpha_1 + 1)(\alpha_2 + 1) \ldots (\alpha_k + 1),$$

$$\zeta(n) = \frac{p_1^{\alpha_1 + 1} - 1}{p_1 - 1} \cdot \frac{p_2^{\alpha_2 + 1} - 1}{p_2 - 1} \cdots \frac{p_k^{\alpha_k + 1} - 1}{p_k - 1}.$$

Even in ancient times (Euclid [85], book VII), the question was raised of finding the numbers n equal to the sum of their proper divisors (i.e. divisors less than n, so that $\zeta(n) = 2n$). Such numbers are called *perfect numbers*. Euclid (book IX) has proved the only theorem known so far on perfect numbers, which states that all *even* perfect numbers are of the form $2^{p-1}(2^p-1)$ when 2^p-1 is a prime. For primality of 2^p-1 it is necessary that the power p is a prime, but this condition is not sufficient. Euler discovered eight values of p for which 2^p-1 is a prime. Namely, $p = 2, 3, 5, 7, 13, 17, 19, 31$ (see Euler [17], vol. I, p. 1 and 584). Corresponding to this, Euler knew eight even perfect numbers. No odd perfect numbers are known, but so far it has not been proved that no such number exists. (See notes to the present chapter.)

Of great importance in the analytical theory of numbers is the *Möbius function* $\mu(n)$ defined for $n = p_1^{\alpha_1}p_2^{\alpha_2}\dots p_k^{\alpha_k}$ as follows: $\mu(n) = 0$ if at least one of the numbers $\alpha_i > 1$; $\mu(n) = (-1)^k$ for $\alpha_1 = \alpha_2 = \dots = \alpha_k = 1$; $\mu(1) = 1$. It is easy to deduce the basic property of $\mu(n)$:

$$\sum \mu(d) = 0 \qquad \text{for } n > 1,$$

where the summation is performed over all the divisors d of number n. From this follows the important *inversion formula*: if for every integer n the function $F(n)$ may be expressed in terms of a function $f(n)$ by formula $F(n) = \sum_{n=d\delta} f(d)$, then, conversely, for every n we have $f(n) = \sum_{n=d\delta} F(d)\mu(\delta)$, where both summations are performed over all divisors d of n, or, in other words, over all the representations of $n = d\delta$ as a product of two positive factors d, δ.

Denote by $\varphi(n)$ the number of integers less than n and prime to n, ($\varphi(1) = 1$). This function was introduced by Euler (see [17], vol. II, p. 127). $\varphi(n)$ is expressed in terms of the prime divisors of n as follows

$$\begin{aligned}\varphi(n) &= p_1^{\alpha_1-1}(p_1-1)p_2^{\alpha_2-1}(p_2-1)\dots p_k^{\alpha_k-1}(p_k-1) \\ &= n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\dots\left(1-\frac{1}{p_k}\right).\end{aligned} \tag{3}$$

I. M. Vinogradov proposed replacing the classical method of proving this formula (L. Dirichlet [14], 11) by the following simpler

one: let $\varepsilon_k^p = 1$ if integer k is divisible by prime p, and $\varepsilon_k^p = 0$ otherwise. Then

$$\varphi(n) = \sum_{m=1}^{n} (1-\varepsilon_m^{p_1})(1-\varepsilon_m^{p_2}) \dots (1-\varepsilon_m^{p_k})$$

$$= n - \sum_{m=1}^{n} \varepsilon_m^{p_1} - \sum_{m=1}^{n} \varepsilon_m^{p_2} - \dots + \sum_{m=1}^{n} \varepsilon_m^{p_1}\varepsilon_m^{p_2} + \dots \pm \sum_{m=1}^{n} \varepsilon_m^{p_1}\varepsilon_m^{p_2} \dots \varepsilon_m^{p_k}$$

$$= n - \frac{n}{p_1} - \frac{n}{p_2} - \dots + \frac{n}{p_1 p_2} + \dots \pm \frac{n}{p_1 p_2 \dots p_k} =$$

$$= n \prod_{r=1}^{k} \left(1 - \frac{1}{p_i}\right).$$

By means of (3) (or directly) the following important property of the function $\varphi(n)$ may be deduced (Gauss [20], D. A., art. 39) [1]:

$$\sum_{n=d\delta} \varphi(d) = n. \tag{4}$$

All the four functions introduced above: $\tau(n)$, $\zeta(n)$, $\mu(n)$ and $\varphi(n)$ satisfy functional equation $f(mn) = f(m)f(n)$ for relatively prime m and n. The functions $\tau(n)$, $\zeta(n)$, $\mu(n)$, $\varphi(n)$ discussed in the present section present elementary *arithmetical* functions, i.e. the quantities defined for an integral argument n. Their changes with increase of argument are very unpredictable. One of these functions, namely $\zeta(n)$ has been studied in more detail because of its connection with the notable Euler's formula for the representation of numbers as a sum of four squares (ch. V, theorems 20 and 23). However, the nature of the other functions $\tau(n)$, $\mu(n)$ and $\varphi(n)$ remains unknown. In subsequent chapters of the present monograph the reader will find many examples of other arithmetical functions.

§ 3. Theorems on the divisibility of factorials

Subsequently $[x]$ denotes the integral part of a real number x (i.e. integer k, defined by conditions $k \leqq x < k+1$) and $\{x\}$ denotes the fractional part of x, i.e. the difference $x - [x]$. In some problems

[1] From now on the initials D.A. denote Gauss's 'Disquitiones Arithmeticae'. For convenience all the references are given to the German translation of this and other works by Gauss in the theory of numbers.

we need to know the power of a given prime p in the standard form of the product $n! = 1 \cdot 2 \cdot 3 \cdots n$. This power (L. Dirichlet [14] § 15) is found to be equal to $[n/p]+[n/p^2]+[n/p^3]+\ldots$. From here we obtain, independently of combinatorial analysis, a proof that the binomial coefficient $(a+b+c+\ldots)!/a!b!c!\ldots$ is an integer, if we calculate the number of times a prime p enters into the numerator and the denominator, and use an obvious property of the sign [ ], namely $[x+y] \geqq [x]+[y]$. In the book 'Niedere Zahlentheorie' [4] by P. Bachmann (part I, p. 57) the reader may find many similar theorems stating that certain expressions in factorials are integers. Among those the Landau theorem is of most interest. Suppose we have two systems of linear forms $f_i(x_1, \ldots, x_n) = a_{i_1}x_1 + \ldots + a_{i_n}x_n$ $(i = 1, 2, \ldots, m)$ and $g_i(x_1, \ldots, x_n) = b_{i_1}x_1 + \ldots + b_{i_n}x_n$ $(i = 1, 2, \ldots, p)$ with non-negative integral coefficients a_{i_j}, b_{i_j}. In order that the expression

$$\frac{f_1(x_1, \ldots, x_n)!f_2(x_1, \ldots, x_n)! \ldots f_m(x_1, \ldots, x_n)!}{g_1(x_1, \ldots, x_n)!g_2(x_1, \ldots, x_n)! \ldots g_p(x_1, \ldots, x_n)!}$$

is an integer for every system of integral non-negative values x_1, $x_2, \ldots, x_n$, it is necessary and sufficient that in the whole domain $0 \leqq y_1 \leqq 1, 0 \leqq y_2 \leqq 1, \ldots, 0 \leqq y_n \leqq 1$ of values of variables y_1, $y_2, \ldots, y_n$, the following inequality is satisfied:

$$\sum_{i=1}^{m} [f_i(y_1, \ldots, y_n)] \geqq \sum_{i=1}^{p} [(g_i(y_1, \ldots, y_n)].$$

§ 4. Theorems of Euler and Fermat; linear congruences

If the difference between two numbers a and b is divisible by number $c \neq 0$, then it is said that *a is congruent to b to modulus c*, which is written as: $a \equiv b \pmod{c}$, or, simply $a \equiv b(c)$. Congruences to the same modulus can be added, subtracted, multiplied and divided by the common factors (when the factor is relatively prime to the modulus). Thus, the operations with congruences are very similar to operations with equations. The congruence sign was introduced by Gauss [20] (D.A., art. 2) and proved to be a very convenient symbol for arithmetical reasonings. Let k be an integer, greater than zero. All the integers congruent to the same integer modulo k form a *class* (the

term 'class' originates from Gauss, Theoria residuorum biquadraticorum, II, art. 42, see [30], p. 551). Since, for every number a we have $a = qk+r$, where r is one of the numbers $0, 1, 2, \ldots, k-1$ and the latter numbers are incongruent modulo k we see that there exist k distinct classes to modulus k. Choosing one representative from each class, we obtain a system of k numbers, which is called a *complete system of residues* to modulus k. For example, numbers $0, 1, 2, \ldots, k-1$ form such a system. If one number of a class is relatively prime to k, then all the numbers of the class possess the same property; there are, obviously, $\varphi(k)$ such classes. Taking one representative from each of these classes we obtain a *reduced system of residues* to modulus k. For example, when k is prime, the numbers $1, 2, \ldots k-1$ form such a system.

Let $(a, k) = 1$ and let x run through a reduced system of residues modulo k, then the products ax are incongruent modulo k, since $ax \equiv ax'$ implies $x \equiv x'$. Moreover, numbers ax are relatively prime to k; consequently, numbers ax are congruent modulo k with numbers x taken in a different order. Multiplying together all the numbers of each set, and comparing the products modulo k, we obtain the important theorem of Euler (sec [17], vol. I, 274)

THEOREM 3. *For every number a relatively prime to a number $k > 0$ the following congruence holds*:

$$a^{\varphi(k)} \equiv 1 \pmod{k}.$$

In particular, if $k = p$ is prime and a is not divisible by p, we have

$$a^{p-1} \equiv 1 \pmod{p}.$$

This theorem is one of the most important ones in the theory of numbers, and was discovered by Fermat. Euler proved it by several methods and generalised it to the case of the composite modulus k.

The reasonings used in the proof of Euler's theorem give another result: a linear congruence $ax \equiv b \pmod{k}$, where a and b are relatively prime to k, has a unique solution for x (considering all the integers of the same class as the same solution). Generalising to the case of arbitrary a and b (L. Dirichlet [14], 22) we obtain the following theorem: for a congruence $ax \equiv b \pmod{k}$ to be possible it is necessary and sufficient that b is divisible by $(a, k) = \delta$, in which case the con-

gruence has δ solutions x incongruent modulo k. The actual evaluation of solutions x of a congruence $ax \equiv b \pmod{k}$ may be performed by using continued fractions employing rule of § 1, since the above congruence is equivalent to an indefinite equation $ax - ky = b$.

To generalise various theorems of the theory of numbers proved for a prime modulus to the case of a composite modulus, we must solve the following problem: find all numbers x satisfying a system of congruences $x \equiv \alpha \pmod{a}, x \equiv \beta \pmod{b}, \ldots x \equiv \gamma \pmod{c}$ where $a, b, \ldots, c$ are positive integers, and $\alpha, \beta, \ldots, \gamma$ are arbitrary integers. Of special importance is the case of moduli $a, b, \ldots, c$ which are co-prime: in this case the above system always has solutions x, where the numbers x form one class modulo $ab \ldots c$ (Dirichlet [14], 25).

When a and a' run through all the numbers of classes K and K' respectively, modulo k, then the product aa' always remains inside one class which we denote by KK'. Denoting by 1 the class which contains number 1, and using the above theorem on linear congruences, we find that for every class K consisting of numbers relatively prime to k there exists a definite class K' ('inverse') such that $KK' = 1$. Thus the system of $\varphi(k)$ classes, into which all the integers relatively prime to k split, satisfies all the definitions of a *finite group*. This group is, clearly, abelian.

§ 5. Theorems of Lagrange and Wilson

Two integral polynomials $P(x)$ and $P_1(x)$ of the form $ax^m + bx^{m-1} + \ldots + c$ are called *congruent* to a prime modulus p if their coefficients of the equal powers of x are congruent modulo p; this is written as $P(x) \equiv P_1(x) \pmod{p}$. If $P(x) \equiv P_1(x)Q(x) \pmod{p}$ where $Q(x)$ is an integral polynomial, then we say that $P(x)$ is *divisible* by $Q(x)$ to modulus p. If $P(x)$ has no other divisors modulo p apart from $aP(x)$ and a (a is an integer $\not\equiv 0 \pmod{p}$), the polynomial $P(x)$ is called *irreducible*, or *prime* to modulus p. Such is, for example every linear polynomial $x + a$. Polynomials prime to modulus p are in complete similarity with ordinary prime numbers, e.g. the following theorem holds: every integral function $A(x)$ of the form $x^m + ax^{m-1} + \ldots$ can be represented modulo p as a product of prime functions

$$A(x) \equiv P_1(x)^{\alpha_1} P_2(x)^{\alpha_2} \ldots P_k(x)^{\alpha_k} \pmod{p}; \tag{5}$$

the representation is unique (polynomials congruent modulo p are not considered distinct). In the congruence (5) $P_1(x)$, $P_2(x)$, ... denote prime polynomials, with the leading coefficient 1, incongruent to modulus p, and numbers $\alpha_1, \alpha_2, \ldots, \alpha_k$ denote positive exponents. This theorem is proved in the same way as the similar one for integers (§ 1). It is performed after establishing the Euclidean Algorithm and finding the properties of the greatest common divisor of two integral polynomials modulo p (see, for example, Bachmann [4], part 1, ch. VII, § 19).

Let $A(x) = a_0x^m + \ldots, a_0 \not\equiv 0(p)$ be an integral polynomial and let the number $x = \alpha$ satisfy the congruence $A(x) \equiv 0 \pmod p$. Dividing $A(x)$ by $x-\alpha$ we obtain $A(x) = (x-\alpha)A_1(x) + A(\alpha) \equiv (x-\alpha)A_1(x) \pmod p$ i.e. $A(x)$ is divisible by a prime polynomial $x-\alpha$ modulo p. Thus, the solution of congruence $A(x) \equiv 0 \pmod p$ is equivalent to separating the linear prime divisors of polynomial $A(x)$ modulo p. Since the number of distinct prime divisors of polynomial $A(x)$ modulo p cannot exceed degree m of this polynomial, we obtain *Lagrange's Theorem*:

THEOREM 4. *A congruence of degree* m, $a_0x^m + a_1x^{m-1} + \ldots + a_m \equiv 0 \pmod p (a_0 \not\equiv 0)$ *cannot have more than* m *incongruent solutions.*

By Fermat's theorem (§ 4), congruence $x^{p-1} - 1 \equiv 0 \pmod p$ has $p-1$ incongruent solutions, therefore the factorisation of $x^{p-1} - 1$ into prime factors modulo p is of the form

$$x^{p-1} - 1 \equiv (x-1)(x-2)\ldots(x-p+1) \pmod p.$$

Comparing the constant terms on both sides, we obtain *Wilson's theorem*: $1.2.3\ldots(p-1) \equiv -1 \pmod p$. This theorem holds for every prime number, and is of special interest, since it expresses a *characteristic* property of primes. In fact, it is obvious that if for some number the expression $1 \cdot 2 \cdot 3 \cdots (p-1)+1$ is divisible by p, then p must be a prime. Combining factors equidistant from both ends in the product $1 \cdot 2 \cdot 3 \cdots (p-1)$, we obtain from Wilson's theorem the congruence $(1 \cdot 2 \cdot 3 \cdots \tfrac{1}{2}(p-1))^2 \equiv (-1)^{\frac{1}{2}(p+1)} \pmod p$ (for $p > 2$) from which, for every prime p of the form $4n+3$, follows the congruence $1 \cdot 2 \cdot 3 \cdots \tfrac{1}{2}(p-1) \equiv \pm 1 \pmod p$. The sign $\pm$ in this congruence is not in a simple relationship with the number p; the problem of this sign was stated by Dirichlet (see [13], vol. 1, p. 107). Since -1

is a quadratic non-residue of a prime p of the form $4n+3$ (see § 8 of this chapter), the congruence

$$1 \cdot 2 \cdot 3 \cdot \cdots \cdot \frac{p-1}{2} \equiv \pm 1 \pmod{p} \tag{6}$$

has + sign if the number β of quadratic non-residues modulo p among the numbers $1, 2, 3, \ldots, \frac{1}{2}(p-1)$ is even, and a $-$ sign if it is odd. Denoting by α the number of quadratic residues among the numbers $1, 2, 3, \ldots, \frac{1}{2}(p-1)$ we have, by Dirichlet's formula (see chapter VI) $\alpha - \beta = h(-p)$ where $h(-p)$ is the number of classes of properly primitive binary forms of determinant $-p$. Combining this with an obvious equality $\alpha + \beta = \frac{1}{2}(p-1)$, we have $\beta = \frac{1}{4}(p+1) - \frac{1}{2}(1+h(-p))$. Thus, the sign in congruence (6) is in relationship with the residue modulo 4 of the quantity $h(-p)$ which varies quite irregularly when p varies. Kronecker used recurrence relationships which he discovered for the number of classes to modify this criterion (see later chapter VI).

§ 6. Primitive roots, indices, binary congruences

Let p be a prime modulus, and let a be a number not divisible by p. Already from Fermat's theorem (§ 4) it is clear that there exist positive indices δ (for example, $\delta = p-1$) for which $a^\delta \equiv 1 \pmod{p}$. If δ the least index of such kind, we say that *a belongs to exponent* δ *modulo* p; this exponent δ must be a divisor of $p-1$, for otherwise $a^\delta \equiv 1$ and $a^{p-1} \equiv 1$, and hence $a^{(\delta, p-1)} \equiv 1 \pmod{p}$ where $(\delta, p-1) < \delta$. A number g belonging to the exponent $\delta = p-1$ is called a *primitive root*. For such a number the powers $1, g, g^2, \ldots, g^{p-2}$ are, clearly, incongruent modulo p and thus they form a reduced system of residues modulo p, since for every $a \not\equiv 0 \pmod{p}$ there exists a power α for which $a \equiv g^\alpha \pmod{p}$. The concept of a primitive root was introduced by Euler (see [17], vol. I, p. 516); however, Euler did not succeed in finding a strict proof of the existence of a primitive root for every prime p. This was first done by Gauss (see [20], D.A. art. 54). Gauss's proof is given below and presents a most brilliant example of arithmetical reasoning. Let $\psi(\delta)$ be the number of integers, incongruent modulo p, belonging to the same exponent δ, a divisor of $p-1$. Suppose there exists at least one such integer, a say, then δ integers $1, a, a^2, \ldots, a^{\delta-1}$

are incongruent modulo p. All these integers satisfy the congruence $x^\delta \equiv 1 \pmod p$, so that the congruence cannot have any other solutions (Theorem 4). Therefore, the remaining integers belonging to the exponent δ(except a) are amongst the powers $1, a, a^2, \ldots, a^{\delta-1}$. Considering a power a^s we find that the exponent d to which it belongs is the smallest integer for which sd is divisible by δ. Therefore, $d = \delta$ if and only if $(s, \delta) = 1$. Thus, for $\psi(\delta) > 0$ we necessarily have $\psi(\delta) = \varphi(\delta)$. Let us split the integers $1, 2, \ldots, p-1$ into classes, collecting into each class the integers belonging to the same exponent δ; a class, corresponding to δ contains $\psi(\delta)$ integers, so that we obtain $\sum \psi(\delta) = p-1$, where the summation is performed over all the divisors δ of $p-1$. Comparing this with a similar relationship for the function φ: $\sum \varphi(\delta) = p-1$ (formula (4)), we find that $\psi(\delta) = \varphi(\delta)$ for every δ, which for $\delta = p-1$ gives Gauss's theorem:

THEOREM 5. *For every prime p there exist $\varphi(p-1)$ primitive roots incongruent modulo p.*

The evaluation of primitive roots for a large p needs lengthy calculations, and is performed by the trial and error method (see [20], D.A. art. 73). P.L. Chebychev (see [82], p. 198) succeeded in finding a primitive root *a priori* for specified moduli p. The simplest Chebychev's theorems are: 1) 3 is a primitive root of a prime p of the form 2^n+1 $(n > 1)$ 2). If a prime p is of the form $p = 4N+1$ where N is a prime $N > 2$, then 2 is a primitive root of p.

If $a \not\equiv 0 \pmod p$, the integer α in the congruence $a \equiv g^\alpha \pmod p$, defined up to a multiple of $p-1$, is called the *index* of a. The system of indices is completely similar to the system of logarithms, since, clearly

$$\operatorname{ind}(ab) \equiv \operatorname{ind} a + \operatorname{ind} b, \qquad \operatorname{ind}\frac{a}{b} \equiv \operatorname{ind} a - \operatorname{ind} b, \pmod{p-1}$$

(a/b denotes the solution of congruence $bx \equiv a \pmod p$). If we succeed in constructing the tables, giving for every integer $1, 2, \ldots, p-1$ its index, and conversely, these tables have the same use in solving congruences, as the tables of logarithms have for ordinary operations. Thus, solution of congruences $ax \equiv b$ and $x^n \equiv A \pmod p$ is reduced to subtraction and division, respectively, to modulus $p-1$. Jacobi

[30] evaluated tables of indices for all primes not exceeding 1000.[1])

Indices are also useful in theoretical reasonings. For example, the problem of solvability of a binary congruence $x^n \equiv A \pmod p$ ($n > 0$ and $A \not\equiv 0 \pmod p$ are given integers) is solved by considering indices and applying to them a known (§ 4) theorem on linear congruences. Thus, let $\delta = (n, p-1)$, for the congruence $x^n \equiv A \pmod p$ to be solvable it is necessary that $A^{(p-1)/\delta} \equiv 1 \pmod p$, in which case the congruence has δ incongruent solutions. This theorem belongs to Euler.

If the congruence $x^n \equiv A \pmod p$ is solvable, then A is called a *residue of degree n*, otherwise it is called a *nonresidue of degree n* for a prime p. It follows from above that A is a residue of degree n if and only if $A^{(p-1)/\delta} \equiv 1 \pmod p$, where $\delta = (n, p-1)$. Considering A in the latter congruence as an unknown and applying to it the theorem on binary congruences, we find that there exist $(p-1)/\delta$ incongruent residues of degree n. The remaining $(\delta-1)(p-1)/\delta$ (for $\delta > 1$) terms of the reduced system of residues are nonresidues of degree n. It seems appropriate to split all nonresidues into $\delta-1$ sets, each containing $(p-1)/\delta$ members, i.e. the same number as there are residues. This is performed as follows. Let r be one of the $\varphi(\delta)$ integers belonging to the exponent δ; since all solutions of the congruence $x^\delta \equiv 1 \pmod p$ are contained in the set $1, r, r^2, \ldots, r^{\delta-1}$ it follows by Fermat's theorem $A^{((p-1)/\delta)\delta} \equiv 1 \pmod p$ that every number $A \not\equiv 0 \pmod p$ satisfies one (and only one) congruence

$$A^{(p-1)/\delta} \equiv r^\alpha \pmod p, \qquad \alpha = 0,1,\ldots,\delta-1.$$

Let us collect into α-th set all the integers A for which the power α of the above congruence is the same. Then: 1) every set consists of $(p-1)/\delta$ members, 2) 0th set consists of residues of degree n, 3) the ratio of two members of the same set is an nth power residue, 4) the product of a member of αth set by a member of βth set belongs to $(\alpha+\beta)$th (or to $(\alpha+\beta-\delta)$th) set. If number r is replaced by another number belonging to exponent δ then only the numeration of sets

[1] Tables of indices are now constructed by J. C. P. Miller and A. E. Western for all primes not exceeding 100000, and for selected values up to 1000000. Western has also evaluated some selected indices up to 6000000. See Royal Society Mathematical tables, volume IX (1968) 'Indices and Residue Indices' by A. E. Western and J. C. P. Miller.

is affected (apart from the zero set). The above sets may also be characterized as follows: members of the same set (to some fixed primitive root) have the same residue modulo δ. For $n = 2, 3, 4$ the residues are called quadratic, cubic and biquadratic.

For a composite modulus k, first consider the case $k = p^\alpha$ where p is an odd prime. In this case there also exist primitive roots, i.e. numbers belonging to the highest possible exponent $\varphi(p^\alpha)$, as it may be easily deduced from theorem 5 (L. Dirichlet [14], § 128). Taking one of them, g say, we may represent the reduced system of residues to modulus $k = p^\alpha$ in the form $1, g, g^2, \ldots, g^{\varphi(k)-1}$. The case $k = 2^\alpha$ is different. The reduced system of residues for this modulus is represented as a cycle for $\alpha = 1$ or 2 only; for $\alpha \geqq 3$ every integer $A \not\equiv 0 \pmod 2$ satisfies $A^{\frac{1}{2}\varphi(k)} = A^{2^{\alpha-2}} \equiv 1 \pmod{2^\alpha}$ and therefore the primitive root does not exist. Taking one of the numbers g_0, belonging to the exponent $2^{\alpha-2}$ (for example, $g_0 = 5$, L. Dirichlet [14], § 130), we may write a reduced system of residues modulo $k = 2^\alpha$ in the form $(-1)^s g_0^t$ where $s = 0, 1$ and $t = 0, 1, \ldots, 2^{\alpha-2}-1$ independently of s. Finally, for a composite number $k = 2^\alpha p_1^{\alpha_1} p_2^{\alpha_2} \ldots$ ($p_1, p_2, \ldots$ are distinct odd primes, $\alpha \geqq 0$, $\alpha_1 > 0$, $\alpha_2 > 0, \ldots$), using theorems on linear congruences to several moduli (§ 4), we find the following composition of a reduced system of residues: $G_{-1}^s G_0^t G_1^{u_1} G_2^{u_2}$, where the exponents $s, t, u_1, u_2, \ldots$ range independently through the complete systems of residues to moduli 2, $\frac{1}{2}\varphi(2^\alpha)$, $\varphi(p_1^{\alpha_1})$, $\varphi(p_2^{\alpha_2}), \ldots$ The numbers G_{-1}, G_0, G_1, G_2 are defined by the following conditions: G_{-1} is absent for $\alpha = 0, 1$; for $\alpha \geqq 2$, $G_{-1} \equiv -1 \pmod{2^\alpha}$, $G_{-1} \equiv 1 \pmod{k/2\alpha}$; number G_0 is absent for $\alpha = 0, 1, 2$; for $\alpha \geqq 3$, $G_0 \equiv g_0 \pmod{2^\alpha}$, $G_0 \equiv 1 \pmod{k/2^\alpha}$; further, $G_1 \equiv g_1 \pmod{p_1^{\alpha_1}}$, $G_1 \equiv 1 \pmod{k/p^{\alpha_1}}$; $G_2 \equiv g_2 \pmod{p_2^{\alpha_2}}$, $G_2 \equiv 1 \pmod{k/p_2^{\alpha_2}}$, etc. Numbers $g_0, g_1, g_2, \ldots$ are selected for separate moduli 2^α, $p_1^{\alpha_1}$, $p_2^{\alpha_2}, \ldots$ to belong to the exponents $\frac{1}{2}\varphi(2^\alpha)$, $\varphi(p_1^{\alpha_1})$, $\varphi(p_2^{\alpha_2}), \ldots$. This theorem from the point of view of group theory provides the fundamental basis for the abelian group of classes of integers relatively prime to k modulo k. (§ 4).

§ 7. Bernoulli numbers

A simple example of an application of the above theorems is provided by *Bernoulli's numbers* $B_1 = \frac{1}{6}$, $B_2 = \frac{1}{30}$, $B_3 = \frac{1}{42}$, which

occur in evaluation of the sums of equal powers of integers. Denoting by x an arbitrary integer greater than zero, and taking $S_k(x) = 1^k + 2^k + \ldots + x^k$, we have

$$\frac{S_{2n}(x)}{x} + (-1)^n B_n = \frac{x^{2n-1}}{2} + \frac{x^{2n}}{2n+1} + \sum_{k=1}^{n-1} (-1)^{k-1} \frac{2n(2n-1)\ldots(2n-2k+2)}{1 \cdot 2 \cdot 3 \cdots 2k} B_k x^{2n-2k}. \tag{7}$$

For $x = 1$ this formula becomes a recurrence relation from which the Bernoulli's numbers may be successively evaluated for $n = 1, 2, 3, \ldots$. The main property of these numbers is presented in the von Staudt's-Clausen's theorem:

THEOREM 6. *Take all primes $p \geqq 2$ for which $p-1$ divides the double suffix $2n$ of Bernoulli's number B_n then*

$$B_n = (-1)^n \sum \frac{1}{p} + \text{an integer}$$

the summation being extended over all the above primes.

Amongst the many proofs of this theorem, the simplest one is the proof by von Staudt himself, which is based on complete induction and does not require any other results apart from formula (7). First, we deduce some properties of sums $S_k(x)$. Let a, b, n be integers greater than zero; noting that each integer $1, 2, \ldots, ab$ is obtained once by formula $x + ay$ where x and y run independently through values $x = 1, 2, \ldots, a$, $y = 0, 1, \ldots, b-1$ we have

$$S_n(ab) = \sum_{x,y} (x+ay)^n \equiv \sum_{x,y} (x^n + nax^{n-1}y) = \\ = bS_n(a) + naS_{n-1}(a)S_1(b-1) \pmod{a^2}. \tag{8}$$

In particular, it follows that $S_n(ab) - bS_n(a) - aS_n(b)$ is divisible both by a and by b. Applying this to relatively prime a and b and then extending to several integers, we may prove that if $a, b, \ldots, l$ are coprime integers, then the expression

$$\frac{S_n(ab\cdots l)}{ab\cdots l} - \frac{S_n(a)}{a} - \frac{S_n(b)}{b} - \ldots - \frac{S_n(l)}{l} \tag{9}$$

is an integer. For an odd v we have

$$2S_v(a) \equiv 2\sum_{x=1}^{a-1} x^v = \sum_{x=1}^{a-1}(x^v+(a-x)^v) \equiv 0 \pmod{a}$$

therefore, replacing in (8) n by $2n$, we have $S_{2n}(ab) \equiv bS_{2n}(a) \pmod{a^2}$. Take $a = p^r$, $b=p$, where $r > 0$ and p is a prime, greater or equal to 2. Then we find that $S_{2n}(p^{r+1})/p^{r+1} - S_{2n}(p^r)/p^r$ is an integer, and therefore $S_{2n}(p^r)/p^r - S_{2n}(p)/p$ is also an integer. Finally, if $2n$ is divisible by $p-1$, then clearly $S_{2n}(p) \equiv -1 \pmod{p}$; if $2n$ is not divisible by $p-1$, then there exists an integer $c \not\equiv 0 \pmod{p}$ for which $c^{2n} \not\equiv 1 \pmod{p}$ (otherwise the congruence $x^{(2n,\,p-1)} \equiv 1 \pmod{p}$, of degree less than $p-1$, allows $p-1$ distinct solutions). Then $c^{2n}S_{2n}(p) \equiv S_{2n}(p) \pmod{p}$, from which $S_{2n}(p) \equiv 0 \pmod{p}$. Thus, for every positive exponent r, one of the numbers $S_{2n}(p^r)/p^r + 1/p$, $S_{2n}(p^r)/p^r$ is an integer, depending on $2n$ being, or being not, divisible by $p-1$. Combining this with the previous remark about expression (8), being an integer, we find, that for every integer x,

$$\frac{S_{2n}(x)}{x} = -\sum\frac{1}{p} + \text{an integer}$$

where the summation is performed over all prime factors p of x for which $2n$ is divisible by $p-1$. Assume now $x = 1 \cdot 2 \cdot 3 \cdots (2n+1)$ $(n \geqq 1)$ in formula (7), and suppose the von Staudt' theorem proved for numbers $B_1, B_2, \ldots, B_{n-1}$. Then the right hand side of (7) is an integer, and $(-1)^n B_n = \sum 1/p + \text{an integer}$, where the summation is taken over all primes p for which $2n \equiv 0 \pmod{p-1}$, i.e. we obtain von Staudt's theorem for number B_n.

Further properties of the Bernoulli numbers are proved in papers by G. F. Voronoy, Kummer and S. Ramanujan [72].

§ 8. Quadratic residues; Gauss's third proof of the quadratic reciprocity law

In a detailed study of quadratic residues, first consider an odd prime modulus p. For such a modulus there exist $\frac{1}{2}(p-1)$ quadratic residues (§ 6) and the same number of quadratic non-residues, the first differing from the latter by a sign + or − in Euler's congruence $A^{\frac{1}{2}(p-1)} \equiv \pm 1 \pmod{p}$. For every $a \not\equiv 0 \pmod{p}$ we denote by the

symbol (a/p) a positive or negative unit according to a being a quadratic residue or a quadratic non-residue of p. The symbol (a/p) was introduced by Legendre. It follows from the results of § 6 that this symbol has the following properties:

$$\begin{aligned} &\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right) \qquad \text{for } a \equiv b \pmod{p} \\ &\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right); \\ &a^{\frac{1}{2}(p-1)} \equiv \left(\frac{a}{p}\right) \pmod{p}. \end{aligned} \tag{10}$$

For which prime moduli p is a a quadratic residue of p? This question interested Euler, who found solutions for $a = -1, \pm 2, \pm 3, \pm 5$ and also guessed the general formula for every prime a. For $a = -1, \pm 2, -3$ the solution of the problem may be seen from the formulae

$$\begin{aligned} &\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2} = \sin\frac{\pi p}{2} \\ &\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8} \\ &\left(\frac{-2}{p}\right) = (-1)^{(p^2-1)/8+(p-1)/2} = \sqrt{2}\sin\frac{\pi p}{4} \\ &\left(\frac{-3}{p}\right) = \frac{2}{\sqrt{3}}\sin\frac{2\pi p}{3} \end{aligned} \tag{11}$$

which may be stated as follows: 1) -1 *is a quadratic residue of primes of the form* $4n+1$ *and a non-residue of primes of the form* $4n+3$; 2) 2 *is a quadratic residue of primes of the form* $8n \pm 1$ *and a quadratic non-residue of primes of the form* $8n \pm 3$ 3) -2 *is a quadratic residue of primes of the form* $8n+1, 8n+3$ *and a non-residue of primes of the form* $8n+5, 8n+7$, 4) -3 *is a quadratic residue of primes of the form* $6n+1$ *and a non-residue of primes of the form* $6n-1$.

The first of these theorems follows from Euler's criterion (see (10)), the third is a consequence of the first, and the fourth follows from the general theorem formulated below. As far as the second theorem is concerned, it may be proved by induction (Gauss [20], D. A. art. 112–114, L. Dirichlet [14] § 41), or it may be deduced from Gauss's

lemma (see below). Let a be equal to an odd prime q. It is remarkable that the answer to the above question (i.e. for what modulus p is q a quadratic residue of p) is in direct relationship with the quadratic character of p modulo q. A theorem expressing this relationship is one of the most important theorems of the theory of numbers; it is called the law of quadratic reciprocity and is formulated as follows:

THEOREM 7. *If at least one of two odd primes p, q is of the form $4n+1$, then $(p/q) = (q/p)$, if both p and q are of the form $4n+3$, then $(p/q) = -(q/p)$. In both cases $(p/q)(q/p) = (-1)^{\frac{1}{2}(p-1)\cdot\frac{1}{2}(q-1)}$.*

As mentioned above, this theorem was discovered by Euler. Legendre formulated it in its present form and succeeded in proving a part of this theorem. The first complete proof of the reciprocity law was given by Gauss [20] (D. A. art 135–144). During his lifetime Gauss has given eight proofs of this theorem based on different principles. Below we give the simplest of these proofs (the third one). Chapter III contains the first Gauss's proof based on the principle of induction.

The third Gauss's proof is based on a lemma which shows, similarly to the Euler's criterion, whether a given number $a \not\equiv 0 \pmod p$ is a quadratic residue or a non-residue of an odd prime p. This lemma is as follows: *Take the absolute least residues of numbers $a, 2a, \ldots, \frac{1}{2}(p-1)a$ modulo p, i.e. the residues lying within the limits $-\frac{1}{2}p, +\frac{1}{2}p$; clearly, none of them is equal to zero. Denoting by μ the number of negative numbers among these residues, we have $(a/p) = (-1)^{\mu}$.* In fact, let $r_1, r_2, \ldots, r_\lambda$ be all the positive and $-s_1, -s_2, \ldots, -s_\mu$ – all the negative among these residues, then r_i and s_j are numbers of the set $1, 2, \ldots, \frac{1}{2}(p-1)$. All the numbers r_i, s_j are distinct, since for $x, y = 1, 2, \ldots, \frac{1}{2}(p-1)$ neither the sum $ax+ay$ nor the difference $ax-ay$ $(x \not\equiv y)$ are divisible by p. Since the number of integers r_i, s_j is equal to $\frac{1}{2}(p-1)$, it is clear that the set of all these integers coincides with the set $1, 2, 3, \ldots, \frac{1}{2}(p-1)$ from which we have

$$(-1)^{\mu} r_1 r_2 \ldots r_\lambda s_1 s_2 \ldots s_\mu$$

$$= (-1)^{\mu} \cdot 1 \cdot 2 \cdots \frac{p-1}{2} \equiv a^{\frac{1}{2}(p-1)} \cdot 1 \cdot 2 \cdots \frac{p-1}{2} \pmod p;$$

and using Euler's criterion, we obtain $(a/p) = (-1)^{\mu}$ q.e.d. From Gauss's lemma we easily obtain the proof of the four theorems formulated above (see (11)); the first three of them are called *auxiliary*

theorems (Ergänzungssätze) to the reciprocity law. Confining ourselves to the second theorem, take $a = 2$ in Gauss's lemma; among numbers $2, 4, \ldots, p-1$ there are $\frac{1}{2}(p-1)-[\frac{1}{4}p]$ numbers with negative least absolute residue modulo p. And it is easy to see that expression $\frac{1}{2}(p-1)-[\frac{1}{4}p]$ is an even integer if $p = 8n+1$ and $8n+7$, and an odd integer if $p = 8n+3$ and $8n+5$.

Returning to the proof of the reciprocity law, we assume a in Gauss's lemma to be an odd prime q, distinct from p. Denoting by $r_1, r_2, \ldots, r_{\frac{1}{2}(p-1)}$ the remainders on division of numbers $q, 2q, \ldots, \frac{1}{2}(p-1)q$ by p, we have

$$q = \left[\frac{q}{p}\right] p + r_1,$$

$$2q = \left[\frac{2q}{p}\right] p + r_2, \ \ldots, \ \frac{p-1}{2} q = \left[\frac{\frac{p-1}{2} q}{p}\right] p + r_{\frac{1}{2}(p-1)}. \tag{12}$$

Denote by A the sum of all numbers r which are less than $\frac{1}{2}p$ and by B the sum of the remaining numbers r (i.e. greater than $\frac{1}{2}p$). In the proof of Gauss's lemma we have seen that the absolute values of the residues of numbers $2q, \ldots, \frac{1}{2}(p-1)q$ taken within the limits $-\frac{1}{2}p$, $+\frac{1}{2}p$, coincide with the set of numbers $1, 2, \ldots, \frac{1}{2}(p-1)$, so that the sum of these absolute values must be equal to $\frac{1}{8}(p^2-1)$. Noting that a residue of xq lying in the interval $-\frac{1}{2}p, +\frac{1}{2}p$ is equal either to r_x or to $r_x - p$ when $r_x < \frac{1}{2}p$ or $r_x > \frac{1}{2}p$, respectively, we obtain

$$\frac{p^2-1}{8} = \mu p - B + A$$

(as before, μ denotes the number of integers r which are greater than $\frac{1}{2}p$). Addition of equalities (12) gives

$$\frac{p^2-1}{8} q = p \cdot [q, p] + A + B$$

where

$$[q, p] = \left[\frac{q}{p}\right] + \left[\frac{2q}{p}\right] + \ldots + \left[\frac{\frac{p+1}{2} q}{p}\right].$$

From these two equalities we have $\frac{1}{8}(p^2-1)(q-1) = ([q,p] - \mu)p + 2B$ from which $\mu \equiv [q,p] \pmod 2$. Consequently, by Gauss's lemma $(q/p) = (-1)^{[q,p]}$ and similarly $(p/q) = (-1)^{[p,q]}$. We now prove that between the two sums $[q,p]$ and $[p,q]$ there exists a relationship

$$[q,p]+[p,q] = \frac{p-1}{2}\cdot\frac{q-1}{2}. \tag{13}$$

Let $q < p$. Then the successive terms in the sum $[q,p]$ cannot differ by more than one; since the last of the latter terms is equal to $[(p-1)q/2p] = [\frac{1}{2}(q-1)+(p-q)/2p] = \frac{1}{2}(q-1)$, the sum $[q,p]$ has terms equal to $0, 1, 2, \ldots, \frac{1}{2}(q-1)$. Let t be one of the numbers $0, 1, \ldots, \frac{1}{2}(q-3)$; the terms $[xq/p]$ of the sum $[q,p]$ which are equal to t satisfy $t < xq/p < t+1$ or $tp/q < x < (t+1)p/q$, so that the number of such terms is equal to $[(t+1)p/q]-[tp/q]$. Noting that there are $\frac{1}{2}(p-1)-[\frac{1}{2}(q-1)p/q]$ terms in sum $[q,p]$ which are equal to $\frac{1}{2}(q-1)$, we find

$$\begin{aligned}
[q,p] &= 1\left(\left[\frac{2p}{q}\right] - \left[\frac{p}{q}\right]\right) + 2\left(\left[\frac{3p}{q}\right] - \left[\frac{2p}{q}\right]\right) + \ldots \\
&\quad + \frac{q-3}{2}\left(\left[\frac{\frac{q-1}{2}p}{q}\right] - \left[\frac{\frac{q-3}{2}p}{q}\right]\right) + \frac{q-1}{2}\left(\frac{p-1}{2} - \left[\frac{\frac{q-1}{2}p}{q}\right]\right) \\
&= \frac{p-1}{2}\,\frac{q-1}{2} - \left(\left[\frac{p}{q}\right] + \left[\frac{2p}{q}\right] + \ldots + \left[\frac{\frac{q-1}{2}p}{q}\right]\right) \\
&= \frac{p-1}{2}\,\frac{q-1}{2} - [p,q],
\end{aligned}$$

which proves formula (13) and with it the reciprocity law.

§ 9. The quadratic character to a composite modulus

Consider solution of the congruence $x^2 \equiv A$ to a composite modulus k, assuming A to be relatively prime to k. If $k = p^\alpha$, where p is an odd prime, then for A to be a quadratic residue modulo p^α (i.e. for a congruence $x^2 \equiv A \pmod{p^\alpha}$ to be possible), it is clearly necessary that A is a quadratic residue modulo p. It is easy to show that this condition is also sufficient (L. Dirichlet [14], § 35) and that if it

holds, the congruence $x^2 \equiv A \pmod{p^\alpha}$ always has two solutions incongruent modulo p^α. Therefore, in a reduced system of residues modulo p^α, half of the terms are quadratic residues, and the remaining half are quadratic non-residues modulo p^α (the same as for a prime modulus). It is not the same for modulus $k = 2^\alpha$. For $\alpha = 2$, in a reduced system of residues $+1, -1$, the number $+1$ is a quadratic residue, and -1 is a quadratic non-residue. For $\alpha = 3$, in a reduced system of residues $\pm 1, \pm 3$ only $+1$ is a residue (since a square of an odd number always is of the form $8n+1$). As far as the higher powers $2^\alpha (\alpha > 3)$ are concerned, it may easily be proved (L. Dirichlet [14], § 36) that a congruence $x^2 \equiv A \pmod{2^\alpha}$ is possible if and only if A is a quadratic residue to modulus 8, i.e. $A \equiv 1 \pmod 8$, in which case the congruence $x^2 \equiv A \pmod{2^\alpha}$ has *four* solutions ($\alpha \geqq 3$). Thus, to modulus $2^\alpha (\alpha \geqq 3)$ a *quarter* of the whole reduced system of residues consists of quadratic residues, and the remaining three quarters – of non-residues. Finally, for any composite modulus $k = 2^\alpha p_1^{\alpha_1} p_2^{\alpha_2} \ldots$ ($\alpha \geqq 0, \alpha_1 > 0, \alpha_2 > 0, \ldots, p_1, p_2, \ldots$ are distinct odd primes) the theorem on linear congruences to several moduli (§ 4) immediately gives conditions of solvability, as well as the number of solutions of congruence $x^2 \equiv A \pmod k$(and of a general congruence $f(x) \equiv 0$ provided it is solvable to moduli of the form p^α). Namely, a congruence $x^2 \equiv A \pmod k$ is possible if and only if $(A/p_1) = (A/p_2) = \ldots = 1$, and $A \equiv 1 \pmod 4$ for $\alpha = 2$, $A \equiv 1 \pmod 8$ for $\alpha \geqq 3$. If these conditions are satisfied, the congruence has $\varepsilon \cdot 2^\nu$ distinct solutions, where ν is the number of primes $p_1, p_2, \ldots$; $\varepsilon = 1$ for $\alpha \leqq 1$, $\varepsilon = 2$ for $\alpha = 2$, and $\varepsilon = 4$ for $\alpha \geqq 3$.

A very useful generalisation of the Legendre's symbol was introduced by Jacobi. Let P be an odd integer, greater than zero, and let m be an integer, relatively prime to P. If $P = pp'p'' \ldots$ is the standard form of P (some factors may repeat), we assume $(m/P) = (m/p)(m/p')(m/p'') \ldots$, where the expressions on the right hand side are Legendre's symbols. Clearly, the symbol (m/p) thus defined has the following properties

$$\left(\frac{m}{P}\right) = \left(\frac{m'}{P}\right) \qquad \text{for } m \equiv m' \pmod P$$
$$\left(\frac{mm'}{P}\right) = \left(\frac{m}{P}\right)\left(\frac{m'}{P}\right), \qquad \left(\frac{m}{PQ}\right) = \left(\frac{m}{P}\right)\left(\frac{m}{Q}\right) \tag{14}$$

Moreover, it is easy to show (L. Dirichlet [14], § 46) that the same law of reciprocity exists for the Jacobi symbol as for Legendre's symbol, with some additional theorems. Namely, for an odd $P > 0$

$$\left(\frac{-1}{P}\right) = (-1)^{\frac{1}{2}(P-1)}, \qquad \left(\frac{2}{P}\right) = (-1)^{(P^2-1)/8},$$
$$\left(\frac{-2}{P}\right) = (-1)^{(P^2-1)/8+(P-1)/2} \tag{15}$$

and for odd, relatively prime $P, Q > 0$

$$\left(\frac{P}{Q}\right)\left(\frac{Q}{P}\right) = (-1)^{\frac{1}{2}(P-1)\cdot\frac{1}{2}(Q-1)}. \tag{16}$$

For convenience of calculations, the Jacobi symbol is extended to the case of a negative denominator, assuming $(m/-P)$ to be (m/P), where, as before, $(m, P) = 1$. Note that the properties of the symbol (m/P) expressed by (14) still hold; in (15) the second equality holds for a negative P, but the rest does not hold. Finally, the reciprocity law (16) holds when and only when one of the P, Q is positive. The practical evaluation of the value of (P/Q) is performed by successive divisions, decreasing the numerator and the denominator of the symbol by means of (14), (15), (16) (see notes to present chapter).

It remains to mention the form of the solution of the problem stated in § 8 (i.e. for which prime moduli p is a given number a a quadratic residue), after the reciprocity law has been proven. For a square-free a we find that all primes p, for which $(a/p) = 1$ are contained in several arithmetical progressions with difference $2|a|$ or $4|a|$. The number of such progressions is equal to $\frac{1}{2}\varphi(2|a|)$ or $\frac{1}{2}\varphi(4|a|)$ (L. Dirichlet [14] § 52).

§ 10. Generalisations of congruences

Consider the generalisations of the concept of congruence. First, let us pause at *congruences to a double modulus* [1] which are very important in the theory of algebraic numbers. Let p be a prime, and let

[1] In other words, the integral functions congruent to a 'double modulus' $(P(x), p)$ form the ideal $Z(x)$ generated by $P(x)$ modulo p. The ideal $Z(x)/p$ is a prime ideal.

$P = x^n + ax^{n-1} + \ldots$ be a polynomial of irreducible *prime* modulo p (§ 5). Two integer polynomials $A(x)$ and $B(x)$ are called *congruent moduli* $(p, P(x))$ if the difference $A(x) - B(x)$ is divisible by $P(x)$ modulo p (§ 5), i.e. if $A(x) - B(x) = P(x)Q(x) + pR(x)$, where $Q(x)$ and $R(x)$ are integral polynomials. This is written as follows: $A(x) \equiv B(x) \pmod{p, P(x)}$. Such congruences, similar to ordinary ones, may be added, subtracted and multiplied. Moreover, a double modulus $(p, P(x))$ has the character of a prime modulus, i.e. $A(x)B(x) \equiv 0 \pmod{p, P(x)}$ implies that one of the functions $A(x)$, $B(x)$ is divisible by modulus $(p, P(x))$. This follows from the fact that $P(x)$ is a prime function modulo p (§ 5). Therefore, both sides of a congruence to a double modulus may be divided by the same polynomial, not divisible by the modulus. The polynomials which congruent modulo $(p, P(x))$ are assumed to belong to the same class; similarity with ordinary modulus extends even to the fact that there is a finite number of such classes. Namely, dividing any polynomial algebraically by $P(x)$, and then taking the residues modulo p of coefficients of the remainder, we deduce that every polynomial is congruent modulo $(p, P(x))$ to one and only one polynomial of the form $ax^{n-1} + bx^{n-2} + \ldots + c$ where $a, b, \ldots, c$ run independently through complete systems of residues modulo p. Thus, the number of distinct classes of polynomials modulis $(p, P(x))$ is equal to p^n. From here we obtain in a usual way the Fermat theorem for a double modulus: for every integral polynomial $A(x)$ the following congruence holds: $A(x)^{p^n} \equiv A(x) \pmod{p, P(x)}$. The generalised Lagrange's theorem should also be noted: a congruence $z^m + A(x)z^{m-1} + B(x)z^{m-2} + \ldots \equiv 0 \pmod{p, P(x)}$ whose coefficients are integral polynomials, has no more than m solutions incongruent modulo $(p, P(x))$.

Congruences to a double modulus enable us to study in more detail prime functions modulo p of a given degree. Assuming in the above Fermat theorem $A(x) = x$ we have $x^{p^n} \equiv x \pmod{p, P(x)}$, i.e. every prime function $P(x)$ of nth degree divides $x^{p^n} - x$ modulo p. Raising congruence $x^{p^n} \equiv x \pmod{p, P(x)}$ several times to power p^n, we find that for every m, divisible by n, we have $x^{p^m} \equiv x \pmod{p, P(x)}$. It is easy to prove the converse to this statement, i.e. that every m for which $x^{p^m} \equiv x \pmod{p, P(x)}$ is divisible by n.

Let for some m, $m = qn + r$, $0 < r < n$; then from $x^{p^m} \equiv x$, $x^{p^n} \equiv x$ we deduce $x^{p^r} \equiv x \pmod{p, P(x)}$. Noting that for a prime p

the binomial coefficient $p!/a!b!\ldots(a+b+\ldots=p, a<p, b<p, \ldots)$ is divisible by p, we have, for every integral polynomial $f(x)$: $f(x^p), \equiv f(x)^p, f(x^{p^2}) \equiv f(x)^{p^2} \ldots f(x^{p^r}) \equiv f(x)^{p^r} \pmod p$, which together with $x^{p^r} \equiv x \pmod{p, Px}$ gives $f(x)^{p^r} \equiv f(x) \pmod{p, P(x)}$. Thus, the congruence $z^{p^r} \equiv z \pmod{p, P(x)}$ is satisfied by every integral polynomial, i.e. this congruence has p^n distinct solutions; but its degree is $p^r < p^n$. Thus the supposition on non-divisibility of m by n contradicts Lagrange's theorem and therefore $m \equiv 0 \pmod n$. Thus, polynomial $x^{p^m}-x$ is divisible modulo p by every prime function whose degree is a divisor of m; $x^{p^m}-x$ has no other divisors. Finally, it is easy to see that none of the above functions enter into the factorisation of $x^{p^m}-x$ with degree higher than one, since otherwise its derivative $p^m x^{p^m-1}-1 \equiv -1 \pmod p$ would be divisible by this function, which is impossible. The above remarks enable us to establish in its final form the factorisation of $x^{p^m}-x$ into prime factors modulo p. Namely, denoting by $\Phi_m(x)$ the product of all distinct functions of mth degree which are prime modulo p, we have

$$x^{p^m}-x \equiv \prod \Phi_d(x) \pmod p \tag{17}$$

where the product is taken over all the divisors d of m. Following Gauss, denote by (n) the number of distinct functions (with leading coefficient 1) of degree n which are prime modulo p. Equating the coefficients of equal powers of x on both sides of (17), we obtain $p^m = \sum d(d)$, from which, by the inversion formula (§ 2), we may express arithmetical function (n) as $(n) = 1/n\sum\mu(d)d^{n/d}$, where the summation is performed over all the divisors of n. The above formula also implies that for every integer $n > 0$ we have $(n) > 0$ (since $\sum\mu(d)p^{n/d}$ cannot be equal to zero, being a sum, or a difference of several distinct powers of a prime p), i.e. there exist prime functions modulo p of any given degree. Finally, applying the inversion formula to (17), we obtain the product of all prime functions modulo p, of a given degree n:

$$\Phi_n(x) \equiv \prod (x^{pn/d}-x)^{\mu(d)} \pmod p,$$

where, clearly, the expression on the right hand side is an integral polynomial in x.

Consider another generalisation of the concept of congruence. Take a system of linear integral forms in n variables $x_1, x_2, \ldots, x_n$:

$$f_i = a_{i1}x_1 + a_{i2}x_2 + \ldots + a_{in}x_n, \quad i = 1, 2, \ldots, n$$

of determinant $d \neq 0$. Two integral linear forms g, g' of the same variables are called *congruent over a system of linear forms* $f_1, f_2, \ldots, f_n$ if the difference $g-g'$ is representable in the form $m_1 f_1 + m_2 f_2 + \ldots + m_n f_n$ where $m_1, m_2, \ldots, m_n$ are rational integers. This is written as $g \equiv g' \pmod{f_i}$. It is important for us to prove the following theorem on these congruences: if all integral linear forms in variables $x_1, x_2, \ldots, x_n$ are split into classes, each class containing all the forms congruent to each other over the system $f_1, f_2, \ldots, f_n$, then the number of such classes is finite; namely, it is equal to $|d|$, i.e. the absolute value of the determinant of the forms $f_1, \ldots, f_n$. (A. Hurwitz [29]). Let k be one of the numbers 1, 2, ..., n. Consider all those integral forms $ax_k + bx_{k+1} + \ldots + cx_n (a \neq 0)$ which are congruent to zero modulo f_i (such forms exist, e.g. dx_k), and choose among them such (or one of such) $g_k = d_k x_k + \ldots + ex_n$ for which d_k has the least positive value. Then in every other form g of the type $g = ax_k + bx_{k+1} + \ldots$, the coefficient a of x_k is divisible by d_k, since otherwise we can select a linear combination $g - hg_k$ (h – an integer) which is congruent to zero modulo f_i and whose coefficient of x_k is greater than zero and less than d_k.

The system of forms $g_1, g_2, \ldots, g_n$ thus constructed has the following property: every integral form F, congruent to zero modulo f_i is representable in the form $m_1 g_1 + m_2 g_2 + \ldots + m_n g_n$ where $m_1, m_2, \ldots, m_n$ are rational integers. In fact, the coefficient of x_1 in form F is divisible by d_1; denoting the result of this division by m_1 we find that the form $F - m_1 g_1$ does not contain x_1 and is $\equiv 0 \pmod{f_i}$. Consequently, the coefficient of x_2 in the form $F - m_1 g_1$ is divisible by d_2; denoting the result of division by m_2, we construct the form $F - m_1 g_1 - m_2 g_2$ etc. From the above property of forms $g_1, g_2, \ldots, g_n$ it follows that all the forms $f_1, f_2, \ldots, f_n$ are expressible as linear integral combinations of forms $g_1, g_2, \ldots, g_n$. But, conversely, since $g_i \equiv 0 \pmod{f_i}$, the forms $g_1, g_2, \ldots, g_n$ are integral linear combinations of forms $f_1, f_2, \ldots, f_n$. Consequently, the determinants of forms $f_1, f_2, \ldots, f_n$ and $g_1, g_2, \ldots, g_n$ may differ in sign only, i.e. $d_1 d_2 \ldots d_n = |d|$. Consider the system of forms $q_1 x_1 + q_2 x_2 + \ldots + q_n x_n$ where $q_1, q_2, \ldots, q_n$ run independently through complete systems of residues to moduli $d_1, d_2, \ldots, d_n$, respectively. From the properties of the forms $g_1, g_2, \ldots, g_n$ it is clear that the forms written above are incongruent modulo f_i. On the other hand, if F is an arbitrary form,

then with a suitable choice of integers $m_1, m_2, \ldots, m_n$ the difference $F - m_1 g_1 - m_2 g_2 - \ldots - m_n g_n$ coincides with one of the forms $q_1 x_1 + q_2 x_2 + \ldots + q_n x_n$, i.e. $F(x) \equiv q_1 x_1 + q_2 x_2 + \ldots + q_n x_n \pmod{f_i}$. Thus, forms $q_1 x_1 + \ldots + q_n x_n$ form a complete system of residues modulo f_i; their number is equal to $d_1 d_2 \ldots d_k = |d|$, q.e.d.

Notes to Chapter 1

§ 1–2

A detailed and systematic exposition of the general theory of numbers can be found in the following textbooks: L. Dirichlet [14, 15], Bachmann [2, 4], Kronecker [36], Landau [38], Legendre [39, 40], Lucas [53], Cahen [9], Borel et Drach [6], St. Smith etc.; in Russian there are books by Chebychev [82] and Grave [22]. Some chapters on elementary theory of numbers are presented in the book by Weber-Wellstein [94].

A historic survey of development of the theory of numbers from ancient times is given in a book by A. V. Vassiliev 'An Integer'. References to all questions on classical theory of numbers with an extensive bibliography may be found in Encyklopädie der Mathematische Wissenschaften (I. Band, II, Teil [16]) and in the three-volumed history of the theory of numbers by Dickson [12].

Other works of encyclopaedic character relating to various branches of the theory of numbers will be referred to in the appropriate places.

Regarding the *length* of the Euclidean algorithm (1) (i.e. the number $n+1$ of divisions, necessary to find the greatest common divisor of two given numbers a, b), the *Chebychev-Lamé* theorem may be easily proved, which states that $n+1 > 5\bar{b}$ where $\bar{b}$ is the number of digits of number b, written in the decimal system. This and other similar theorems the reader may find in a book by Bachmann [4] (p. 114 and following).

A nearest generalisation of Euclid's theorem on unboundedness of the series of primes is the famous Dirichlet theorem, which states that *in every arithmetical progression $ax+b$ where a and b are relatively prime, and $a > 0$, there exists an infinite number of primes.* A general proof of this theorem requires the analysis of infinitesimals (see, for example, L. Dirichlet [14] suppl. VI). In some particular cases, how-

ever, for example for a progression $ax \pm 1$ the proof may be performed elementarily (see Landau [37], p. 436 and following. I. Schur [78]). *

Factorisation of a large number into prime factors is a problem which interested greatly the old mathematicians (Fermat, Euler, Gauss). In every factorisation of N into two factors one of the factors is less or equal to $\sqrt{N}$, therefore to find out whether N is a prime or a composite number, N must be divided by all primes less than $\sqrt{N}$.

When N is large this involves a great deal of calculation. If, however, N is of some special form (for example a^k+b^k, x^2+y^2, x^2+2y^2 etc.), then from the theory of power residues (§§ 4, 6, ch. I), and the theory of quadratic forms (§ 8, ch. II and ch. IV), we may find out *a priori* the form of the prime divisors of N and thus reduce considerably the number of trials.

For example, by Fermat's theorem (§ 4) if p is a prime, then the prime divisors of 2^p-1 must be of the form $2px+1$; thus Euler verified the fact that the numbers of the form 2^p-1 given in the text are prime. Recently, the interest in the latter problem has been revived in connection with Fermat's last theorem (see notes to § 4), and with some other problems. Especially one should note the papers of the American mathematician D. H. Lehmer [41, 42, 44, 45] who evaluated detailed tables of primes, and constructed several machines which simplify the factorisation of numbers (i.e. decomposition into prime factors). One of Lehmer's computors is in the institute of Physical Mathematics of the Academy of Sciences, U.S.S.R. In particular, concerning numbers of the form 2^p-1 where p is a prime, on which depends the finding of even perfect numbers and which, for $p \leqq 257$ are called Mersenne numbers (Lucas [53], p. 376), the present day position is as follows [1] (see Lehmer [41, 44], Western [97]): 1). It is established that 2^p-1 is a prime [2] for $p = 2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127$; 2) the complete factorisation of these numbers [3] is known for $p = 11,$

---

[1] At present there are 23 known Mersenne primes, for $p = 2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127, 521, 607, 1279, 2203, 2281, 3217, 4253, 4423, 9689, 9941, 11213$.

[2] The number $2^{11213}-1$ has 3376 digits and is the greatest prime known.

[3] The complete factorisation of 2^p-1 is known for $p = 11, 23, 29, 37, 41, 43, 47, 53, 59, 67, 71, 73, 79, 83, 97, 101, 103, 109, 113, 131, 151, 163, 179, 181$.

* See Wojceck: A refinement of a theorem of Schur on primes in arithmetical progressions. Acta Arithmetica 11 :1966; 433–436.

23, 29, 37, 41, 43, 47, 53, 59, 67, 71, 73; 3) one or more prime factors of 2^p-1 are known [1] for $p = 79^*, 83^*, 97^*, 113^*, 131, 151^*, 163^*, 173^\dagger, 179^*, 181^*, 191^\dagger, 197^\dagger, 211^\dagger, 223^\dagger, 233, 239, 251^\dagger$; 4). It is established that 2^p-1 is composite for $p = 101, 103^*, 109, 137, 149, 257$; 5) nothing that is known for powers [2] $p = 157^*, 167^\dagger, 193^*, 199^{**}, 227^{**}, 229^\dagger, 241^*$.

In the theory of the division of the circle of great importance are the primes of the form 2^k+1. Namely, Gauss has proved (see [20], D. A., VII. Abschn.) that the circle may be divided into a prime number p of equal parts by ruler and compass if and only if p is of the form 2^k+1. Clearly, 2^k+1 can only be a prime if $k = 2^n$. For $n = 0, 1, 2, 3, 4$ the numbers $p = 2^{2^n}+1$ are, in fact, prime, which gave Fermat the reason for supposing that for further values of n the expression $2^{2^n}+1$ is giving prime values. However, for $n = 5$ Euler (see

---

* The complete factorisation is known. † One or more factors established.

** Composite but no factor known.

[1] The following results are available on the factorisation of 2^p-1 into prime factors

R. M. Robinson examined factors $q < 2^{30}$ of 2^p-1 for

$$101 \leqq p \leqq 157$$

(see Math. Comp. Vol. 11, 1957, pp. 265–268)

John Brillhart and C. D. Johnson ('On the factors of certain Mersenne numbers' Math. Comp. vol 14, 1960, p. 365–369) sought prime factors q for the numbers $M_p = 2^p-1$ for primes $p < 1200$ in the intervals indicated:

$p = 101$	$2^{30} < q < 2^{35}$
$103 \leqq p \leqq 157, p \neq 151,$	$2^{30} < q < 2^{31}$
$157 < p \leqq 257$	$1 < q < 2^{31}$
$257 < p \leqq 1021, p \neq 397$	$1 < q < 2^{30}$
$p = 397$	$1 < q < 2^{32}$
$1021 < p < 1200$	$1 < q < 2^{28}$

Later J. Brillhart (Math. Comp. vol. 18, 1964, p. 87–95) discovered 899 new factors, which combined with previous results in the literature constitute all primes $q < 2^{35}$ of M_p with

$$103 \leqq p \leqq 257$$

and all $q < 2^{34}$ of Mp with

$$257 < p < 20000.$$

Sidney Kravitz and Joseph Madachy (Math. Comp. vol. 21, 1967) have computed all prime factors $q < 2^{25}$ of Mersenne numbers for $20000 < p < 1000000$.

No factor of $2^{65537}-1$ is known.

[2] No factors are known for 137, 139, 149, 199, 227, 257, 271, 293, 331, 347, 349, 379, 503, 523, 541, 563, 599, 613, 631, 647, 661, 677, 691, 727, 733, 739, 751, 769, 787, 797, 809, 823, 919, 971, 983, 991, 997, 1061, 1063, 1069, 1109, 1123, 1151, 1163, 1171.

[17], vol. I, p. 1) has discovered the divisibility of $2^{2^n}+1$ by 641. Later, various authors have found that $2^{2^n}+1$ is a composite number [1] for $n = 6, 9, 11, 12, 18, 25, 36, 38$ (Lehmer [44]). For other methods of factorisation of numbers see notes to § 8, ch. II.

Similar to perfect numbers are *amicable* numbers, which have been studied extensively by Euler. Two numbers m, n are called amicable if each of them is equal to the sum of the proper divisors of the other, so that $\zeta(m)+\zeta(n) = m+n$. Such are, for example numbers $m = 2^2 \cdot 71$ and $n = 2^2 \cdot 5 \cdot 11$. In the memoir 'De numeris amicabilibus' (see [17], v. I, p. 102) Euler gives the table of 61 pairs [2] of amicable numbers.

The proof of formula (3) for function $\varphi(n)$ and of theorem on a non-residue of power e of a prime number (§ 8, ch. II) were kindly communicated to me by Academician I. M. Vinogradov, and are taken from the recent edition of his lectures on the theory of numbers.

Many formulae are known, containing various transformations of elementary nature of arithmetical functions $\varphi(n)$, $\tau(n)$, $\mu(n)$ and some formulae are easily deduced from the main properties of these functions listed in § 2; the most interesting of which is Smith's formula

$$\begin{vmatrix} (1,1) & (1,2) & \dots & (1,n) \\ (2,1) & (2,2) & \dots & (2,n) \\ \dots & \dots & \dots & \dots \\ (n,1) & (n,2) & \dots & (n,n) \end{vmatrix} = \varphi(1)\varphi(2)\dots\varphi(n),$$

where (a, b) denotes, as always, the greatest common divisor of a and b. Such formulae are found in a book by Bachmann [4]; for more recent literature see papers by Lehmer [48] and Schröder [77].

§ 4. The Fermat's theorem presented in this section is called *the little Fermat's theorem* to distinguish it from the *Fermat's great last theorem* which states that $z^n = x^n + y^n$ cannot be solved in positive or the

---

[1] At present it is known that $2^{2^n}+1$ is composite for $n = 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 18, 19, 21, 23, 26, 27, 30, 32, 36, 38, 39, 42, 52, 55, 58, 63, 73, 77, 81, 117, 125, 144, 150, 207, 226, 228, 250, 267, 268, 284, 316, 452, 1945$.

[2] More pairs of amicable numbers may be found in E. B. Escott 'Amicable numbers', Scripta Math. vol. 12, 1946, pp. 61–78, P. Poulet '43 new couples of amicable numbers' Scripta Math. vol. 14, 1948, p. 77.

M. Garcia 'New amicable pairs' Scripta Math. vol. 23, 1957, pp. 167–171, 264 new pairs of amicable numbers are given in: Amicable numbers and the Bilinear Diophantine equation' Math. Computation vol. 22 No. 101, 1968.

integers x, y, z for $n > 2$. This theorem was formulated by Fermat without any proof and still has not been proved completely (i.e. for every $n > 2$). It is mainly famous by the amount of effort which is put into attempts to prove it, both by specialists and the amateurs of the theory of numbers alike. For $n = 3$ and 4 this theorem was proved by Euler, for $n = 5$ by Dirichlet, for all $n \leqq 100$ by Kummer who connected it with Bernoulli's numbers (see notes to § 7). At present the theorem is proved for all $n < 307$. *

The number $q(a) = (a^{p-1}-1)/p$, which is an integer for prime p and a not divisible by p (by Fermat's theorem) is called the *Fermat quotient*. The study of the residue of this number modulo p is important for the proof of the Fermat's last theorem, since attempts to prove this theorem have led to congruences of the type $2^{p-1} \equiv 1$, $3^{p-1} \equiv 1$ etc. i.e. to congruences $q(2) \equiv q(3) \equiv 0 \pmod{p}$. From the known expressions for Fermat's quotients we note Stern's form $q(2) \equiv 1+\frac{1}{3}+\frac{1}{5}+\ldots+1/(p-2) \pmod{p}$ where $1/k$ denotes the root of the congruence $xk \equiv 1 \pmod{p}$ (see Bachmann [4], part I, p. 164). The table of values of $q(2)$ for primes $p < 1000$ is in a textbook by Grave [22].

§ 5. Unpublished manuscripts of A. N. Korkine, which are kept in the Institute of Mathematics and Physics, Academy of Sciences, U.S.S.R., give a method for determining the $\pm$ sign in the congruence (6) for a prime $p \equiv 3 \pmod{4}$. This method is based on the following statement, which may easily be proved: the congruence (6) has a + sign if the number $\frac{1}{4}(p-3)+[\sqrt{p}]+[\sqrt{2p}]+\ldots+[\sqrt{((p-3)/4)p}]$ is even, and – sign if the number is odd. Korkine gives a method for the successive construction of numbers $[\sqrt{p}]$, $[\sqrt{2p}]$, ... by means of additions only, which is similar to Jean Bernoulli's method (see § 13, ch. II). For the application of this method we must first evaluate several first terms of the series $[\sqrt{p}]$, $[\sqrt{2p}]$, ..., not more than $(p+21)/36$ in number. However, it seems that in practice Korkine's method leads to more complicated calculations than the Kronecker's criterion (see § 2, ch. VI).

§ 6. In the memoirs 'Sur la distribution des résidues et des non-résidues des puissances' (1918), 'On the distribution of indices' [88]

* Translator's note:
Fermat's last theorem is true for all exponents $n < 25000$. See J. L. Selfridge and B. W. Pollack, Notices Amer. Math. Soc. 1964.

(1926) and 'Some theorems on the distribution of indices and primitive roots' [89] (1933) Academician I. M. Vinogradov has given approximation theorems on the distribution of primitive roots and indices in a progression, which is similar to his theorem on the distribution of power residues (§ 2, ch. III). His method is elementary; it consists of estimating the module of several trigonometrical sums. In Vinogradov's 1918 memoirs a theorem is proved which is described here in chapter III (see end of § 2, ch. III); incidentally, from this theorem it follows that the least primitive root of a prime p does not exceed $2^{\nu}((p-1)/\varphi(p-1))\sqrt{p}\log p$.* From this it is deduced that the number of elementary operations, which are necessary to obtain a primitive root of a prime p is the quantity of order of magnitude $p^{\frac{1}{2}+3/\log\log p}$. In Vinogradov's 1926 memoirs the following theorem is proved: *let $p>3$ be a prime, let $c=hf>2$ be a divisor of $p-1$, let α be integers relatively prime to p, f and let b, β be any integers; finally let p_1, f_1 be integers satisfying $0<p_1\leqq p$, $0<f_1\leqq f$. Then the number of pairs x, y $(x=0, 1, \ldots, p_1-1, y=0, 1, \ldots, f_1-1)$ satisfying the congruence* $\operatorname{Ind}(ax+b)\equiv h\alpha y+\beta \pmod{c}$ *is equal to* $p_1f_1/c+\theta\sqrt{p}\log p\log c$, *where* $|\theta|<1$. In Vinogradov's 1933 memoirs the following theorem is proved: *Let $p>19$, $0<U<p$, $0<V<p$, r and $s\not\equiv 0 \pmod{p}$ and let x run through a reduced system of residues modulo p. Then the number of values of x for which both x and $rx+s$ are primitive roots of p and also satisfy* $0<\operatorname{ind}x\leqq U$, $0<\operatorname{ind}(rx+s)\leqq V$ *(indices are taken to a fixed primitive root, and the value of x for which $rx+s\equiv 0 \pmod{p}$ is excluded), is just* $UV(\varphi(p-1)/(p-1))^2/(p-1)+\theta\cdot 2^{\nu+1}\sqrt{p}\,(\log p)^2$ *where ν is the number of distinct prime divisors of $p-1$* and $|\theta|<1$. The recent papers of I. M. Vinogradov [90, 92](1934) study the number of cases when three numbers x, $x+q$, $x+s$ $(x=1, 2, \ldots, p-1)$ are simultaneously primitive roots, and other similar problems.

For the practical solution of *binary congruences*, A. N. Korkine [33] has given a method, based on the introduction of certain auxiliary numbers, which he calls *characters*, and which may be evaluated once and for all for a given prime modulus. Korkine's method is especially useful since K. A. Posse [70, 71] has extended the calculation of the tables of characters up to 10000. The detailed proof of

* This result has now been improved by L. A. Burgess, who showed that the least primitive root is $O(p^{\frac{1}{4}+\varepsilon})$; see L. A. Burgess, Proc. London Math. Soc. 1962, 179–192.

Korkine's method is in his memoirs, cited above [33] and also in Grave's [22] book which contains extracts from the tables of characters up to 2000.

§ 7. The Bernoulli numbers have acquired a special importance for the proof of Fermat's last theorem (see note to § 4), following Kummer's proof in 1850 of the following theorem: *equation* $x^p+y^p+z^p=0$ *has no solution in integers if prime* $p>2$ *does not divide Bernoulli's numbers* $B_1, B_2, \ldots, B_{\frac{1}{2}(p-3)}$. The exposition on Kummer can be found in volume III of Landau's [38] book.

§ 8. As has been mentioned in the text, Gauss gave eight distinct proofs of the quadratic reciprocity law. Of these the first and the third are given in the text, the second is based on the theory of quadratic forms, the fourth – on the study of the so-called Gaussian sums, the fifth – on Gauss's lemma (see text), the sixth – on the theory of the division of the circle, seventh and eights – on the study of the congruences of higher degree. Later authors gave 50 new proofs of this theorem. However in these proofs no *essentially* new principles are used, and all of them present more or less masked propositions of Gaussian proofs. Analysis of almost all existing proofs of the reciprocity law, together with a detailed historical and literal references, can be found in Bachmann's [4] book (part I, ch. VI).

The identity (13), proved in the text (which is true for every two odd relatively prime numbers p, q) has, as it was noted by Eisenstein, a simple geometrical interpretation. Marking on the plane four points O, A, B, C with coordinates $(0, 0)$, $(\frac{1}{2}p, 0)$, $(0, \frac{1}{2}q)$, $(\frac{1}{2}p, \frac{1}{2}q)$, respectively, we easily find that $[q, p]=[q/p]+[2q/p]+\ldots+[\frac{1}{2}(p-1)q/p]$ is the number of points with integral coordinates, lying within the triangle OAC; similarly $[p, q]$ is the number of such points inside triangle OBC. On the other hand, it is evident that inside the rectangle $OACB$ there lie in all $\frac{1}{2}(p-1)\cdot\frac{1}{2}(q-1)$ such points, which gives formula (13). There exist other interesting identities similar to (13). For example, $\sum_{x=1}^{\frac{1}{2}(q-1)}[px/q+\frac{1}{2}]=\sum_{x=1}^{\frac{1}{2}(p-1)}[qx/p+\frac{1}{2}]$ (see Bachmann [4], Stieltjes [80], vol. II, p. 567). Here belongs also the following theorem, proved by Stieltjes in his memoirs 'Sur la loi de réciprocité de Legendre' (see [80], vol. II, p. 567). If we denote by D the point of intersection of the diagonals of rectangle $OACB$, then inside the triangles ADC and BDC there are the same number of integral points. An elegant geometrical proof of this theorem was

reported by a student of the Leningrad State University, M. M. Artjukhov at the S. U. congress of mathematicians in Leningrad (June, 1934). Another formula similar to (13) is

$$h\sum_{\mu=1}^{k-1}\mu\left[\frac{h\mu}{k}\right]+k\sum_{\nu=1}^{h-1}\nu\left[\frac{k\nu}{h}\right]=\tfrac{1}{12}(h-1)(k-1)(8hk-h-k-1)$$

($h>0$, $k>0$ are relatively prime), which is important in the Dedekind's theory of modular functions. *

§ 9. Useful practical rules for the evaluation of the Jacobi symbol (P/Q) by means of the Euclidean algorithm and by means of the algorithms similar to it, are given by Gauss, Zeller, Eisenstein, Kronecker etc. (see Bachmann [4], part I, ch. VI). The simplest of these is the *Eisenstein rule*: take, successively $P=qQ+\varepsilon_1 Q_1$, $Q=q_1Q_1+\varepsilon_2Q_2,\ldots,$ $Q_{k-1}=q_kQ_k+\varepsilon_{k+1}Q_{k+1}$ where $Q, Q_1,\ldots,Q_{k+1}=1$ are decreasing odd numbers; $q, q_1,\ldots,q_k$ are even numbers greater or equal to 2, and $\varepsilon_1,\varepsilon_2,\ldots\varepsilon_{k+1}$ are equal to ±1. Then try to find the number λ of times that Q_ν and $\varepsilon_{\nu+1}Q_{\nu+1}$ $(\nu=0,1,\ldots,k)$ are simultaneously $\equiv 3 \pmod 4$. Then $(P/Q)=(-1)^\lambda$.

§ 10. A similar exposition on the theory of congruences to a double modulus $(p, P(x))$ is given in Bachmann's [4] book (part I, ch. VII). The question of the solution of linear congruences with many variables is studied in detail (by means of so called *theory of elementary divisors*) in an unfinished work by Stieltjes 'Sur la théorie des nombres' (see [80], vol. II, pp. 265–377 see also Bachmann, Die Arithmetik der quadratischen Formen [3] (II. Abschn. III Kap.)

---

* For a simple arithmetical proof see L. J. Mordell. The reciprocity formula for Dedekind sums Amer. J. Math. 13 (1951).

2. CONTINUED FRACTIONS AND DIOPHANTINE APPROXIMATIONS

Diophantine approximations are the approximations of a given number by means of a *rational* number (integral or fractional), or, more generally, solutions of various inequalities in integers. Diophantine approximations are obtained by means of the following three elementary tools: Farey series, the Dirichlet principle, and continued fractions. In the present chapter we shall consider each one of these tools with a degree of thoroughness corresponding to the breadth of their application.

§ 1. Farey series

Let n be an integer greater than zero. Let us write the ascending series of irreducible fractions between 0 and 1 whose numerators and denominators do not exceed n. Adjoining to them the fractions 0/1 and 1/1, we obtain the so called *Farey series of order n*. The main property of these series is the following: *if a/b and a'/b' are two successive terms of a Farey series, then $a'b-ab' = 1$*. We prove this property by induction, and at the same time obtain a convenient method for constructing the Farey series. The theorem is true for the Farey series of order one: 0/1, 1/1. Supposing the theorem true for the Farey series of order n, we deduce that it is true for the Farey series of order $(n+1)$. Let a/b , a'/b' be two consecutive fractions of the Farey series of order n; then $b+b' > n$, since otherwise an irreducible fraction $(a+a')/(b+b')$, lying between a/b and a'/b' also belongs to the series of order n. From this it is easy to deduce the following method for constructing the Farey series of order $(n+1)$: in the series of order n, take all the pairs a/b, a'/b' of consecutive terms such that $b+b' = n+1$, and separate each such pair by the fraction $(a+a')/(b+b')$. This gives the Farey series of order $(n+1)$. In fact, every term of the constructed series is an irreducible proper fraction with denominator not exceeding

$(n+1)$. On the other hand, let s/t be a fraction satisfying $(s, t) = 1$, $0 < s < t = n+1$. Since s/t does not belong to the Farey series of order n we have $a/b < s/t < a'/b'$, where a/b and a'/b' are two consecutive terms of this series. If s/t differs from $(a+a')/(b+b')$ then it lies in one of the intervals $(a/b, (a+a')/(b+b'))$, or $((a+a')/(b+b'), a'/b')$. Each of these intervals is of the form $(\alpha/\beta, \gamma/\delta)$ where $\gamma\beta-\alpha\delta = 1$, and hence, by a known proposition (see next paragraph), the denominator of s/t must exceed β and δ, i.e. $t > b+b' \geqq n+1$, which is impossible, since $t = n+1$. Therefore, $s/t = (a+a')/(b+b')$. Consequently, the series constructed above is the Farey series of order $(n+1)$. Clearly, the theorem is true for the constructed series, i.e. it is true for the Farey series of order $(n+1)$.

The proposition used above may be proved as follows: if s/t is an irreducible fraction such that $\alpha/\beta < s/t < \gamma/\delta$, $\beta, t, \delta > 0$, $\gamma\beta-\alpha\delta = 1$, then $s/t-\alpha/\beta < 1/\beta\delta$, $t/\delta > s\beta-t\alpha \geqq 1$. Consequently, $t > \delta$ and similarly $t > \beta$.

Concerning the question: how accurately can a given number be approximated by a rational fraction? We should point out the following *Dirichlet theorem*, due to its simplicity and many applications.

THEOREM 8. (L. Dirichlet [14], § 141) *Let ω and $\tau \geqq 1$ be real numbers; there exists an irreducible fraction p/q satisfying the following conditions*

$$\left|\omega - \frac{p}{q}\right| < \frac{1}{\tau q}, \qquad 0 < q \leqq \tau$$

By means of the Farey series this theorem is proved as follows: Let $0 \leqq \omega < 1$ and let $n = [\tau]$; enclose ω between two consecutive terms of Farey series of order n: $a/b \leqq \omega < a'/b'$. Then $p/q = a/b$ for $a/b \leqq \omega \leqq (a+a')/(b+b')$, and $p/q = a'/b'$ for $(a+a')/(b+b') < \omega < a'/b'$. In fact, clearly $0 < q \leqq \tau$; further $|\omega-p/q| \leqq 1/q(b+b') \leqq 1/q(n+1) < 1/\tau q$ q.e.d.

Let ω be an irrational number $0 < \omega < 1$. Then ω falls in an interval bounded by two consecutive fractions $a_n/b_n, a'_n/b'_n$ of the Farey series of order n. Taking $n = 1, 2, 3, \ldots$ we obtain the sequence of fractions

$$\frac{a_1}{b_1}, \frac{a'_1}{b'_1}; \quad \frac{a_2}{b_2}, \frac{a'_2}{b'_2}; \quad \frac{a_3}{b_3}, \frac{a'_3}{b'_3}; \ldots, \tag{1}$$

giving approximations to ω from both sides, where approximations improve when n increases. Properties of series (1) as well as their connection with simple continued fractions, were investigated by Hurwitz [26]; whose results are partially reproduced in the book by Bachmann [4] (part. I, p. 125 and the following).

§ 2. The Dirichlet principle. Theorems of Kronecker and Minkowski

If a number of objects has to be distributed into n places, where the number of objects is greater than n, then there exists a place containing at least two objects. This proposition, which Dirichlet very ingeniously applied to proofs of Diophantine inequalities, is called the *Dirichlet principle*. (H. Minkowski [59], Kap. I). Using this principle we prove the following theorem of Kronecker, which generalises theorem 8: *Let n, t be integers greater than zero, and let $\omega_1, \omega_2, \ldots, \omega_n$ be any real numbers; there exist integers $z, x_1, x_2, \ldots, x_n$ satisfying the following conditions*:

$$|\omega_1 z - x_1| < \frac{1}{t}, \quad |\omega_2 z - x_2| < \frac{1}{t}, \ \ldots, |\omega_n z - x_n| < \frac{1}{t},$$
$$0 < z \leqq t^n. \tag{2}$$

Let q run through numbers $0, 1, 2, \ldots, t^n$. Define for every q a system of integers $p_1, p_2, \ldots, p_n$ satisfying

$$0 \leqq \omega_1 q - p_1 < 1, \quad 0 \leqq \omega_2 q - p_2 < 1, \ \ldots, \ 0 \leqq \omega_n q - p_n < 1. \tag{3}$$

These conditions define $p_1, p_2, \ldots, p_n$ uniquely for a given q. In an n-dimensional space consider a domain consisting of points $(y_1, y_2, \ldots, y_n)$ satisfying the conditions

$$0 \leqq y_1 < 1, \quad 0 \leqq y_2 < 1, \ \ldots, \ 0 \leqq y_n < 1. \tag{4}$$

Introducing into every interval $(0, 1)$ the fractions $1/t, 2/t, \ldots, (t-1)/t$ we split this domain into t^n domains of the form

$$\frac{k_1}{t} \leqq y_1 < \frac{k_1+1}{t}, \ \ldots, \ \frac{k_n}{t} \leqq y_n < \frac{k_n+1}{t}; \tag{5}$$
$$k_1 = 0, 1, \ldots, t-1; \ \ldots; \ k_n = 0, 1, \ldots, t-1.$$

By (3) the point with coordinates $\omega_1 q - p_1, \ldots, \omega_n q - p_n$ belongs to

domain (4), and therefore it falls into one (and only one) of domains (5). But the number of such points is equal to the number of values of q, i.e. t^n+1, whilst the number of domains (5) is t^n. Consequently, by the Dirichlet principle, at least one domain (5) contains two distinct points (i.e. points corresponding to distinct q). Denoting by $q', p_1', \ldots, p_n'$ and $q'', p_1'', \ldots, p_n''$ the values of $q, p_1, \ldots, p_n$ corresponding to these points where $0 \leqq q' < q'' < t^n$, and denoting $q''-q' = z, p_1''-p_1' = x_1, \ldots, p_n''-p_n' = x_n$, we obtain inequalities (2) for numbers $z, x_1, \ldots, x_n$.

If at least one of the numbers $\omega_1, \ldots, \omega_n$ is irrational, then it follows from Kronecker's theorem that there exists an infinite number of systems of fractions $x_1/z, \ldots, x_n/z$ satisfying

$$\left|\omega_1 - \frac{x_1}{z}\right| < z^{-1-1/n}, \ldots, \left|\omega_n - \frac{x_n}{z}\right| < z^{-1-1/n}.$$

Minkowski [60] found an important theorem which contains the theorems of Dirichlet and Kronecker as particular cases. Minkowski's theorem is the following:

THEOREM 9. *Let* $f_i = a_{i1}x_1 + a_{i2}x_2 + \ldots + a_{in}x_n (i = 1, 2, \ldots, n)$ *be a system of n linear forms in n variables with real coefficients, whose determinant* $d \neq 0$. *If* $\lambda_1, \ldots, \lambda_n$ *are positive numbers satisfying* $\lambda_1 \lambda_2 \ldots \lambda_n = |d|$, *then we may find for* $x_1, \ldots, x_n$ *integer values, not simultaneously zero such that*

$$|f_1| \leqq \lambda_1, \quad |f_2| \leqq \lambda_2, \ldots, |f_n| \leqq |\lambda_n|.$$

Minkowski himself has proved his theorem by geometrical methods. Hilbert and Hurwitz have given proofs based on the Dirichlet principle. Recently, Mordell [62] has given a proof which is close in its idea to Hurwitz's proof. We follow Hurwitz's proof which is the simplest. Replacing forms f_i by forms $(\sqrt[n]{|d|}/\lambda_i)f_i$ with the same determinant d we see that our problem is equivalent to the following: indicate the integer values for variables $x_1, \ldots, x_n$ not simultaneously zero, for which the absolute value of every given form $f_i = a_{i1}x_1 + \ldots + a_{in}x_n$ does not exceed $\sqrt[n]{|d|}$. Suppose first that the coefficients a_{ij} of given forms are *integers*, not all zero. Consider a system of forms $\bar{f}_i = a_{1i}x_1 + a_{2i}x_2 + \ldots + a_{ni}x_n (i = 1, 2, \ldots, n)$ whose matrix of coefficients is obtained from the corresponding matrix of forms f_i by interchanging rows and columns. $\bar{f}_1, \ldots, \bar{f}_n$ is a sys-

tem of integral forms with the same determinant d. According to § 10, Chapter I, there exist exactly $|d|$ integral linear forms in variables $x_1, x_2, \ldots, x_n$ which are incongruent with respect to the system $f_1, \ldots, f_n$. Take $r = [\sqrt[n]{|d|}]$ so that $r^n \leqq |d| < (r+1)^n$. Then among $(r+1)^n$ forms $k_1x_1+k_2x_2+\ldots+k_nx_n$ ($k_1 = 0, 1, \ldots, r; \ldots; k_n = 0, 1, \ldots, r$) whose number is greater than $|d|$, there must be two forms congruent modulo f_i. Let $m_1x_1+\ldots+m_nx_n$ be the difference of these forms; then $|m_i| \leqq r \leqq \sqrt[n]{|d|}$ and $m_1x_1+\ldots+m_nx_n = x_1^0f_1+x_2^0f_2+\ldots+x_n^0f_n$ where $x_1^0, \ldots, x_n^0$ are integers, not simultaneously zero. Comparing in this equation the coefficients of $x_1, \ldots, x_n$ and taking into account inequalities for m_i, we find that for the system of values $x_1 = x_1^0, \ldots, x_n = x_n^0$ we have:

$$|f_1| \leqq \sqrt[n]{|d|}, \quad |f_2| \leqq \sqrt[n]{|d|}, \ldots, |f_n| \leqq \sqrt[n]{|d|} \tag{6}$$

which proves the theorem for the integral forms f_i. Since inequalities (6) are homogeneous with respect to the coefficients of the given forms f_i, it follows immediately that the theorem is also true for forms f_i with *rational coefficients* a_{ij}.

For forms f_i with arbitrary real coefficients, the theorem is proved by means of limits. Let $\varepsilon_k (k = 1, 2, \ldots)$ be a sequence of positive numbers, tending to zero. For every k take a system of forms $f_i^{(k)}$ with rational coefficients $a_{ij}^{(k)}$ which differ from the corresponding coefficients of the given forms by less than ε_k. Denoting by d_k the determinant of forms $f_i^{(k)}$, we have $a_{ij}^{(k)} \to a_{ij}$, $d_k \to d$ when $k \to \infty$ hence, for all sufficiently large k, $d_k \neq 0$. Since the theorem is true for forms $f_i^{(k)}$, there exists a system of integer values $x_1, \ldots, x_n$, not all zero, for which

$$|f_1^{(k)}| \leqq \sqrt[n]{|d_k|}, \ldots, |f_n^{(k)}| \leqq \sqrt[n]{|d_k|}. \tag{7}$$

Solving inequalities (7), we find that the values $x_1, \ldots, x_n$ satisfying these inequalities are contained within limits which do not widen indefinitely as $k \to \infty$. Consequently, these limits may be considered as independent of numbers ε_k. Their precise evaluation is not needed. But there exist only a finite number of distinct systems of integers $x_1, \ldots, x_n$ contained within definite limits, and therefore in the inequalities (7) the same system of numbers $x_1, \ldots, x_n$ is repeated for an infinite number of values of k. Passing to limits, we find that this system of numbers satisfies inequalities (6) which, proves Minkowski's theorem.

Further study of Minkowski's theorem and its applications is found in Minkowski's books 'Geometrie der Zahlen [60] and 'Diophantische Approxiomationen' [59].

§ 3. The Hermite theorem

In his letters to Jacobi, Hermite (see Hermite [2], p. 103) has formulated the following theorem: *Given any quadratic form* $F = \sum a_{ij} x_i x_j (a_{ij} = a_{ji}, i, j = 1, 2, \ldots, n)$ *with real coefficients* a_{ij} *and determinant* $d \neq 0$, *there exist integers* $x_1, \ldots, x_n$, *not all zero, such that the numerical value of* F *is less than* $\varepsilon_n \sqrt[n]{|d|}$. Here ε_n depends only on n, and not on the coefficients of the form. Hermite takes $\varepsilon_n = (\frac{4}{3})^{(n-1)/2}$ and conjectures that it may be reduced to $2/\sqrt[n]{n+1}$.*

Let $F = \sum_{i=1}^{n} p_i f_i^2$ where $f_1, \ldots, f_n$ are linear forms of variables $x_1, \ldots, x_n$, with real coefficients and determinant 1, and let $p_1, p_2, \ldots, p_n$ be positive or negative numbers connected by the relation $p_1 p_2 \ldots p_n = d$. Denoting by $\lambda_1, \lambda_2, \ldots, \lambda_n$ arbitrary positive numbers whose product is equal to one, we may find by Minkowsky's theorem, the integer values for $x_1, \ldots, x_n$, not all zero, for which $|f_1| \leqq \lambda_1, \ldots, |f_n \leqq \lambda_n$ and, consequently, $F \leqq \sum_{i=1}^{n} |p_i| \lambda_i^2$. It remains to select for $\lambda_1, \lambda_2, \ldots, \lambda_n$ values (connected by the condition $\lambda_1 \lambda_2 \ldots \lambda_n = 1$) for which the right hand side of the above inequality is the smallest. This is clearly so when all the terms of the sum $\sum |p_i| \lambda_i^2$ are equal to each other and, consequently, each is equal to $\sqrt[n]{|d|}$. Thus, we obtain $|F| \leqq n \sqrt[n]{|d|}$ i.e. the Hermite theorem with a constant $\varepsilon_n = n$.

The *precise* upper limits of the minima of quadratic forms in n variables for integer values of the variables have been determined for *positive forms* for $n = 2, 3, 4, 5$ by Korkine and Zolotareff (see [98], ser. I, pp. 7, 66, 109, 375), and for *indefinite* forms for $n = 3, 4$, they are given by A. A. Markov [55, 56]. We shall consider only the case $n = 2$. If a quadratic form $f = ax^2 + 2bxy + cy^2 = (a, b, c)$ is transformed by substitution $x = \alpha x' + \beta y'$, $y = \gamma x' + \delta y'$ into form $f' = a'x'^2 + 2b'x'y' + c'y'^2$ then the coefficients a', b', c' are given by

$$a' = a\alpha^2 + 2b\alpha\gamma + c\gamma^2$$
$$b' = a\alpha\beta + b(\alpha\delta + \beta\gamma) + c\gamma\delta$$
$$c' = a\beta^2 + 2b\beta\delta + c\delta^2$$

* For footnote see page 242.

This substitution will be denoted by $\left(\begin{smallmatrix}\alpha & \beta\\ \gamma & \delta\end{smallmatrix}\right)$. The number $d = b^2-ac$ (the determinant of form f) is connected with the corresponding determinant d' of f' by relation $d' = d\varepsilon^2$ where $\varepsilon = \alpha\delta-\beta\gamma$. If f transforms into f' by substitution $S = \left(\begin{smallmatrix}\alpha & \beta\\ \gamma & \delta\end{smallmatrix}\right)$, and f' transforms into f'' by substitution $S' = \left(\begin{smallmatrix}\alpha' & \beta'\\ \gamma' & \delta'\end{smallmatrix}\right)$, then f is transformed into f'' by substitution $SS' = \left(\begin{smallmatrix}\alpha\alpha'+\beta\gamma' & \alpha\beta'+\beta\delta'\\ \gamma\alpha'+\delta\gamma' & \gamma\beta'+\delta\delta',\end{smallmatrix}\right)$ which is called the *product* of transformations S and S'.

If the coefficients of substitution $\left(\begin{smallmatrix}\alpha & \beta\\ \gamma & \delta\end{smallmatrix}\right)$ transforming f into f' are integers, then in Gauss's terminology f *contains* f'. In this case every number representable by form f' with integer values of the variables x', y' is also representable by form f with x, y integers. Finally, if integers α, β, γ, δ are connected by relation $\alpha\delta-\beta\gamma = \pm 1$, then the forms f, f' have the same discriminant, and each of them contains the other, so that the systems of numbers representable by these forms with integer values of the variables coincide. Forms f and f' are then called *equivalent*. All these definitions, which belong to Gaussian theory of quadratic forms (see chapter IV) can be easily extended to forms with an arbitrary number of variables.

Let k be an integer. Substitution $\left(\begin{smallmatrix}0 & -1\\ 1 & k\end{smallmatrix}\right)$ transforms form $f = (a, b, c)$ into form $f' = (c, -b+kc, a-2kb+ck^2)$. We call f' a *right neighbouring* form to f (contigua a parte ultima by Gauss). The dependence between f and f' for $c \neq 0$ may be characterised as follows, $f = (a, b, c)$ and $f' = (c, b', e)$ have the same determinant and $(b+b')/c$ is an integer. Similarly, a form $'f = (e', b', a)$ having the same determinant as $f = (a, b, c)$ and such that $(b+b')/a$ is an integer is called a *left neighbouring* form to f (contigua a parte prima). Clearly, the form $f' = (c, b', e)$, which is a right neighbouring form to $f = (a, b, c)$ may be selected in such a way that the absolute value of its middle coefficient does not exceed $\frac{1}{2}c$.

Let $f = (a, b, a')$ be a binary form with arbitrary real coefficients. First suppose that f is a *positive* form, i.e. $a > 0$, $a' > 0$, $d = b^2-aa' < 0$. We construct a *chain* of forms

$$(a, b, a'), (a', b', a''), (a'', b'', a'''), \ldots \tag{8}$$

each of which is a right neighbouring form to the previous one. Coefficients of these forms are chosen by the following condition: $|b'| \leqq \frac{1}{2}a', \ldots, |b^{(n)}| \leqq \frac{1}{2}a^{(n)}, \ldots$.

Clearly, each form of the chain (8) is equivalent to the first

form $(a, b, a') = f$. We assert that this chain contains a form $(a^{(n)}, b^{(n)}, a^{(n+1)})$ for which $a^{(n)} \leqq a^{(n+1)}$. In fact, otherwise $a' > a'' > a''' > \ldots$ which is impossible, since a'', a''', ... are values taken by form f for some integral arguments, whilst a positive form f can take only a finite number of values less than a''. Therefore, for every positive form f we may select an equivalent form $(a^{(n)}, b^{(n)}, a^{(n+1)}) = (A, B, C)$ whose coefficients satisfy the conditions $|2B| \leqq A \leqq C$. The latter are the so called *Lagrange conditions for a form to be reduced.* From $|d| = AC - B^2$ we find $|d| \geqq \frac{3}{4}A^2$ from which $A \leqq \sqrt{\frac{4}{3}|d|}$. Therefore: *for every positive binary form f of determinant d we may find integer values of variables, not simultaneously zero, such that* $f \leqq \sqrt{\frac{4}{3}|d|}$. This limit is precise, since a form $\sqrt{\frac{4}{3}|d|}(x^2+xy+y^2)$ of determinant d cannot be made less than $\sqrt{\frac{4}{3}|d|}$ for integral x, y which are not simultaneously zero.

If f is an indeterminate form, i.e. $d = b^2 - aa' > 0$ we exclude the case when f is zero for some pair of integer values not both zero. Then in the form f (and in every form equivalent to it) the outside coefficients are not equal to zero. Under this supposition on form f the following theorem holds: *the variables x, y may be given integer values, not simultaneously zero, for which* $|f| \leqq \sqrt{\frac{4}{5}d}$. This limit is, again, *precise*, since the form $\sqrt{\frac{4}{5}d}(x^2+xy-y^2)$ of determinant d clearly has a minimum $\sqrt{\frac{4}{5}d}$ (for integral x, y). The formulated theorem (belonging to A. N. Korkine [98], vol. II, p. 332) is proved later (§ 4, ch. IV).

§ 4. Continued fractions. The properties of convergents

Now consider the third tool for obtaining the Diophantine approximations – continued fractions. The algorithm of continued fractions has occupied a notable place in the works of Euler and Lagrange on the number theory; the first has discovered, and the second has proved the most important property of this algorithm – the periodicity of a continued fraction obtained in the development of a quadratic irrationality. The detailed exposition of all the results in the theory of continued fractions until 1912, together with references in the literature, are found in the book by O. Perron, Die Lehre von den Kettenbrüchen [69]. We shall only be concerned with *simple* continued fractions, i.e. the expressions of the form

$$a_1+\cfrac{1}{a_2+\cfrac{1}{a_3+\ddots}} = [a_1, a_2, a_3, \ldots] \tag{9}$$

in which a_1 is an arbitrary integer, and $a_2, a_3, \ldots$ are positive integers. These integers are called the *partial quotients*, (*Teilnenner*) or simply the *quotients* of the fraction (9). Expressions

$$\frac{P_0}{Q_0} = \frac{1}{0}, \quad \frac{P_n}{Q_n} = [a_1, a_2, \ldots, a_n], \qquad n = 1, 2, 3, \ldots$$

are called *convergents* to (9). Their numerators and denominators are evaluated from the expressions

$$P_0 = 1,\ Q_0 = 0;\quad P_1 = a_1,\ Q_1 = 1;\quad P_{n+1} = a_{n+1}P_n + P_{n-1},$$
$$Q_{n+1} = a_{n+1}Q_n + Q_{n-1}, \qquad n = 1, 2, 3, \ldots \tag{10}$$

From these expressions the following properties of P_n and Q_n may easily be deduced:

$$\begin{aligned} P_nQ_{n-1} - P_{n-1}Q_n &= (-1)^n \\ P_{n+1}Q_{n-1} - P_{n-1}Q_{n+1} &= (-1)^n a_{n+1} \end{aligned} \qquad n = 1, 2, 3, \ldots \tag{11}$$

$$\begin{aligned} \frac{Q_n}{Q_{n-1}} &= [a_n, a_{n-1}, \ldots, a_2] \qquad n = 2, 3, \ldots \\ \frac{P_n}{P_{n-1}} &= [a_n, a_{n-1}, \ldots, a_1] \qquad n = 1, 2, \ldots \end{aligned} \tag{12}$$

From (10) we deduce that $0 < Q_1 \leqq Q_2 < Q_3 < Q_4 < \ldots$ whilst $Q_1 = Q_2$ only for $a_2 = 1$. It follows from (11) that: 1) every convergent P_n/Q_n is an irreducible fraction; 2) with increase of n the odd convergents increase, and even convergents decrease; 3) every even convergent is greater than any odd convergent. If a continued fraction is finite, then its value, coinciding with the value of its last convergent, is equal to a rational number. Conversely, every rational number x may be developed into a finite continued fraction. For this we may use the Euclidean Algorithm (ch. I, § 1); this algorithm gives for x a continued fraction $[a_1, a_2 \ldots, a_n]$ in which $a_n > 1$. Since the latter fraction may be written as $[a_1, a_2, \ldots, a_{n-1}, 1]$ we see that x may be expressed as a continued fraction in just two ways, one with an even and the other with an odd number of convergents.

Let $x = [a_1, a_2, \ldots]$ be a continued fraction, finite or infinite, assume

$$x = a_1 + \cfrac{1}{a_2 + \cfrac{\cdot}{\cdot + \cfrac{\cdot}{\cdot + a_k + \cfrac{1}{x_k}}}} = [a_1, a_2, \ldots, a_k, x_k], \; k = 1, 2, 3, \ldots$$

The number $x_k = [a_{k+1}, a_{k+2}, \ldots]$ is called the *complete quotient*. This number is connected with x by a relation

$$x = \frac{P_k x_k + P_{k-1}}{Q_k x_k + Q_{k-1}} \tag{13}$$

from which, using (11), we obtain the following useful formulae

$$x - \frac{P_k}{Q_k} = \frac{(-1)^{k-1}}{Q_k(Q_k x_k + Q_{k-1})}, \quad x_k = -\frac{Q_{k-1}x - P_{k-1}}{Q_k x - P_k}$$

$$x_1 x_2 \ldots x_k = \frac{(-1)^k}{P_k - Q_k x}, \qquad k = 1, 2, 3, \ldots \tag{14}$$

The last of these formulae belongs to H. J. S. Smith. Formulae (14) give

$$\begin{aligned} &\left| x - \frac{P_k}{Q_k} \right| < \frac{1}{Q_k^2}, \quad |Q_k x - P_k| < |Q_{k-1}x - P_{k-1}|, \\ &\left| x - \frac{P_k}{Q_k} \right| < \left| x - \frac{P_{k-1}}{Q_{k-1}} \right|, \qquad k = 1, 2, 3, \ldots \end{aligned} \tag{15}$$

In these inequalities for *rational* x the inequality sign may sometimes be replaced by $=$ sign; namely, in the first inequality when x is an integer and $k = 1$; in the second for $x_k = 1$ and arbitrary k; in the third – when $x + \frac{1}{2}$ is an integer and $k = 2$.

Every *irrational* real number x can be developed in just one way as an *infinite* continued fraction; on the other hand, it is easy to see that every infinite continued fraction is irrational. From (14) and (15) it is evident that for irrational x every odd convergent is less than x, and every even convergent is greater than x; moreover $P_k/Q_k \to x$ as $k \to x$. Take two neighbouring convergents P_{n-1}/Q_{n-1}, P_{n+1}/Q_{n+1} ($n \geqq 1$) of the same parity; they are the first and the last in the series of fractions

$$\frac{R_n^\mu}{S_n^\mu} = \frac{P_{n-1} + \mu P_n}{Q_{n-1} + \mu Q_n}, \qquad \mu = 0, 1, 2, \ldots, a_{n+1} \tag{16}$$

These fractions (for $0 < \mu < a_{n+1}$) are called *intermediate* fractions between P_{n-1}/Q_{n-1} and P_{n+1}/Q_{n+1}. From

$$\frac{R_n^{\mu+1}}{S_n^{\mu+1}} - \frac{R_n^{\mu}}{S_n^{\mu}} = \frac{(-1)^n}{S_n^{\mu} S_n^{\mu+1}}, \quad \frac{R_n^{\mu}}{S_n^{\mu}} - \frac{P_n}{Q_n} = \frac{(-1)^{n-1}}{Q_n S_n^{\mu}}$$

it is evident that the fractions R_n^{μ}/S_n^{μ} are irreducible and go from P_{n-1}/Q_{n-1} to P_{n+1}/Q_{n+1} as n increases (i.e. increase for even n and decrease for odd n).

The convergent P_k/Q_k with denominator $Q_k > 1$ is the *best* approximation to number x in the sense that it represents this number more accurately than any fraction with smaller denominator; namely, if integers a, b are such that $|x-a/b| \leqq |x-P_k/Q_k|$ and $0 < b \leqq Q_k$, then $a = P_k$, $b = Q_k$. In fact, for $a/b \neq P_k/Q_k$ the fraction a/b falls inside the segment P_k/Q_k, P_{k-1}/Q_{k-1} which implies $b > Q_k$. The convergents do not exhaust all the best approximations (in the sense of our definition). We may show that this property is possessed also by those intermediate fractions of series (16) for which $2\mu \geqq a_{n+1}$. Moreover, for $2\mu = a_{n+1}$ the fraction R_n^{μ}/S_n^{μ} is the best approximation if and only if $Q_n/Q_{n-1} < x_{n+1}$, or, in other words, when $[a_n, a_{n-1}, \ldots, a_2] < [a_{n+2}, a_{n+3}, \ldots]$. There are no other best approximations to a given number. This rule (realised already by Huyghens) has been proved by H. J. S. Smith.

The above properties of convergents make it easy to prove again theorem 8 of § 1 of the present chapter. Moreover, we shall see in the next section that in certain cases the accuracy of the approximation given in theorem 8 may be improved by using the convergents.

§ 5. The Legendre criterion; the theorems of Vahlen and Borel

Legendre ('Essai sur la théorie des nombres' [39] p. 20) has given a criterion for a given irreducible fraction $p/q (q > 0)$ to be a convergent to a given number x. Assuming $p/q \neq x$, we assume $x-p/q = \theta/q^2$ and develop p/q into a continued fraction with even number of convergents if $\theta < 0$, or with odd number of covergents if $\theta > 0$. Let p'/q' be the convergent preceding the last. *In order that p/q is a convergent to x it is necessary and sufficient that* $|\theta| \leqq q/(q+q')$. In fact, if $x = [a_1, a_2, a_3, \ldots]$ and $p/q = P_k/Q_k$, then taking $x_k = [a_{k+1}, a_{k+2}, \ldots]$, we have by (14)

$$x - \frac{p}{q} = \frac{(-1)^{k-1}}{q(qx_k + Q_{k-1})} = \frac{\theta}{q^2}, \tag{17}$$

from which $\theta \cdot (-1)^{k-1} > 0$, i.e. the expansion $p/q = [a_1, \ldots, a_k]$ coincides with the above mentioned development of p/q into a continued fraction. Consequently, $Q_{k-1} = q'$ and (17) gives $|\theta| = q/(qx_k + q') \leqq q/(q+q')$. Conversely if the inequality $|\theta| \leqq q/(q+q')$ is satisfied, denote by $[a_1, a_2, \ldots, a_k]$ the above development of p/q into a continued fraction, so that $p'/q' = [a_1, \ldots, a_{k-1}]$ and $pq' - p'q = (-1)^k$. Defining x_k from equation $x = (px_k + p')/(qx_k + q')$ we have $\theta q^2 = (-1)^{k-1} q(qx_k + q')$, $|\theta| = q/(qx_k + q')$, $qx_k + q' > 0$, and from inequality $|\theta| \leqq q/(q+q')$ we obtain $x_k \geqq 1$. Combined with $x = [a_1, a_2, \ldots, a_k, x_k]$ this shows that x_k is a complete quotient, and that p/q is a convergent in the development of x, q.e.d. Since $q' \leqq q$, the Legendre inequality $|\theta| \leqq q/(q+q')$ is definitely satisfied if $|\theta| \leqq \frac{1}{2}$ i.e. if $|x - p/q| \leqq 1/2q^2$. Thus, *if* $|x - p/q| \leqq 1/2q^2$, *then* p/q *is a convergent to* x. This remark leads to the following question: how frequently do convergents p/q occur in the continued fraction for x, which differ from x by less than $1/2q^2$. The answer to this question is given in the Vahlen's theorem [84]: *Of two convergents* P_k/Q_k, P_{k+1}/Q_{k+1}, $(k > 1)$ *at least one satisfies inequality* $|x - p/q| < 1/2q^2$.

The convergents P_k/Q_k, P_{k-1}/Q_{k+1} lie on different sides of x; therefore, if we had

$$\left| x - \frac{P_k}{Q_k} \right| \geqq \frac{1}{2Q_k^2}, \quad \left| x - \frac{P_{k+1}}{Q_{k+1}} \right| \geqq \frac{1}{2Q_{k+1}^2}$$

then we would have $|P_{k+1}/Q_{k+1} - P_k/Q_k| = 1/Q_k Q_{k+1} \geqq 1/2Q_k^2 + 1/2Q_{k+1}^2$ or $(Q_{k+1} - Q_k)^2 \leqq 0$, $Q_{k+1} = Q_k$ which is impossible for $k > 1$. The theorem is proved.

An even greater degree of accuracy of a convergent is achieved in the Borel theorem: *of three consecutive convergents* P_k/Q_k, P_{k-1}/Q_{k-1}, $P_{k-2}/Q_{k-2} (k > 0)$ *at least one satisfies inequality*

$$\left| x - \frac{p}{q} \right| < \frac{1}{\sqrt{5}q^2} \tag{18}$$

For otherwise from $|x - P_i/Q_i| \geqq 1/\sqrt{5}Q_i^2 (i = k, k+1, k+2)$, and from (14) we would have

$$x_k+\frac{Q_{k-1}}{Q_k}\leqq\sqrt{5},\quad x_{k+1}+\frac{Q_k}{Q_{k+1}}\leqq\sqrt{5},\quad x_{k+2}+\frac{Q_{k+1}}{Q_{k+2}}\leqq\sqrt{5}. \tag{19}$$

First two of these inequalities, on replacing x_k by $a_{k+1}+1/x_{k+1}$ give for $u=x_{k+1}>1$ and $v=Q_{k+1}/Q_k\geqq 1$ the following results: $v+1/u\leqq\sqrt{5}$, $u+1/v\leqq\sqrt{5}$. From which

$$\frac{1}{v}\leqq\sqrt{5}-u,\quad v\geqq\frac{1}{\sqrt{5}-u},\quad \frac{1}{\sqrt{5}-u}+\frac{1}{u}\leqq\sqrt{5},\quad u^2-\sqrt{5}u+1\leqq 0,$$

$$u\leqq\frac{\sqrt{5}+1}{2}$$

and, by symmetry $v\leqq(\sqrt{5}+1)/2$. Thus,

$$x_{k+1}\leqq\frac{\sqrt{5}+1}{2},\quad \frac{Q_{k+1}}{Q_k}\leqq\frac{\sqrt{5}+1}{2}. \tag{20}$$

Similarly, the last two inequalities of (19) give

$$x_{k+2}\leqq\frac{\sqrt{5}+1}{2},\quad \frac{Q_{k+2}}{Q_{k+1}}\leqq\frac{\sqrt{5}+1}{2}. \tag{21}$$

From (20) and (21) we find, consecutively: $a_{k+2}=1$, $Q_{k+2}/Q_{k+1}=1+Q_k/Q_{k+1}\leqq\frac{1}{2}(\sqrt{5}+1)$, $Q_{k+1}/Q_k\geqq\frac{1}{2}(\sqrt{5}+1)$, which, together with (20) gives an impossible result: $Q_{k+1}/Q_k=\frac{1}{2}(\sqrt{5}+1)$. Borel's theorem is proved.

§ 6. Equivalent numbers

Two real numbers x, x' are said to be *equivalent*, if they are connected by a relation $x'=(\alpha x+\beta)/(\gamma x+\delta)$ where α, β, γ, δ are integers and $\alpha\delta-\beta\gamma=\pm 1$. It is easy to see that two numbers equivalent to a third are equivalent to each other, and that two rational numbers are always equivalent.

For irrational numbers the following Serret's theorem holds (see [79], pp. 34–37): *Two numbers x and x' are equivalent if and only if their continued fractions, starting from some places, give the same sequence of quotients.* The sufficiency of the condition follows from the fact that x is equivalent to every complete quotient in its development into a continued fraction. To prove the necessity, assume x and x' to be

equivalent, i.e.

$$x' = \frac{\alpha x+\beta}{\gamma x+\delta}, \quad \alpha\delta-\beta\gamma = \pm 1, \tag{22}$$

and let x_n denote a complete quotient of x, so that $x = [a_1, a_2, \ldots, a_n, x_n] = (P_n x_n+P_{n-1})/(Q_n x_n+Q_{n-1})$. Substituting this expression for x into (22) we find $x' = (ax_n+b)/(cx_n+d)$ where

$$\begin{aligned} &a = \alpha P_n+\beta Q_n, \quad b = \alpha P_{n-1}+\beta Q_{n-1}, \quad c = \gamma P_n+\delta Q_n, \\ &d = \gamma P_{n-1}+\delta Q_{n-1}, \qquad ad-bc = \pm 1. \end{aligned} \tag{23}$$

Let us prove that for a sufficiently large n, integers c, d satisfy the condition $0 < d < c$. In fact, the number $\gamma x+\delta$ (which is not equal to zero) may be assumed to be positive, since otherwise we can change signs of all numbers $\alpha, \beta, \gamma, \delta$ which does not change the relation (22). Since $d/Q_{n-1} = \gamma P_{n-1}/Q_{n-1}+\delta \to \gamma x+\delta$ when $n \to \infty$, we have $d > 0$ for all $n \geqq \nu$. Noting that $c = a_n d+(\gamma P_{n-2}+\delta Q_{n-2})$, we find that $c > d > 0$ for $n \geqq \nu+1$. The fraction a/c is irreducible by (23); developing it into a continued fraction $a/c = [a'_1, a'_2, \ldots, a'_k]$ whose number k of quotients satisfies $ad-bc = (-1)^k$, we obtain the following formulae for the convergent a'/c' preceding the last:

$$\begin{aligned} ac'-ca' &= (-1)^k = ad-bc, \\ a(d-c') &= c(b-a'), \\ d-c' &\equiv 0 \pmod{c} \end{aligned}$$

and since $0 < d < c$, $0 < c' < c$ we have $c' = d$, $a' = b$. Therefore,

$$x' = \frac{ax_n+a'}{cx_n+c'} = [a'_1, a'_2, \ldots, a'_k, x_n] = [a'_1, \ldots, a'_k, a_{n+1}, a_{n+2}, \ldots]$$

q.e.d.

Serret's theorem enables us to enlarge upon the theory of approximations to a number x by means of convergents of the continued fraction which expresses it. It follows from Borel's theorem that for every irrational x there exists an infinite number of fractions p/q satisfying inequality (18). First, let us note that $\sqrt{5}$ in this inequality is a *precise* limit in the sense that there exist irrational numbers x_0 for which $|x_0-p/q| < 1/\varepsilon q^2$ is satisfied only by a limited number of fractions p/q for every $\varepsilon > \sqrt{5}$. Take, for example, $x_0 = \frac{1}{2}(\sqrt{5}+1) = [1, 1, 1, \ldots]$; then every complete quotient is equal to $\frac{1}{2}(\sqrt{5}+1)$.

By Legendre's criterion (§ 5) all the fractions p/q satisfying

$$\left| x_0 - \frac{p}{q} \right| < \frac{1}{\varepsilon q^2} \tag{24}$$

are found among the convergents to x_0. If $p/q = P_k/Q_k$, then from (24) we find

$$x_k + \frac{Q_{k-1}}{Q_k} = \frac{\sqrt{5}+1}{2} + \frac{Q_{k-1}}{Q_k} > \varepsilon. \tag{25}$$

But by (12) $Q_k/Q_{k-1} = [1, 1, \ldots, 1]$($k-1$ ones) and, consequently, $Q_k/Q_{k-1} \to x_0$, $Q_{k-1}/Q_k \to 1/x_0 = \frac{1}{2}(\sqrt{5}-1)$ when $k \to \infty$. Therefore, for $\varepsilon > \sqrt{5}$ inequality (25) is satisfied only by a limited number of suffixes k. Clearly, the same reasonings apply to any number x_0 which is equivalent to $\frac{1}{2}(\sqrt{5}+1)$. But for numbers which are not equivalent to $\frac{1}{2}(\sqrt{5}+1)$, the limit $\sqrt{5}$ in inequality (18) may be raised; namely, the following theorem holds: *for every irrational number x not equivalent to $\frac{1}{2}(\sqrt{5}+1)$ there exists an infinity of fractions p/q satisfying inequality*

$$\left| x - \frac{p}{q} \right| < \frac{1}{2\sqrt{2}q^2}.$$

If the theorem is false, then, developing x into a continued fraction, we have for all $k \geqq v$

$$\left| x - \frac{P_k}{Q_k} \right| \geqq \frac{1}{2\sqrt{2}Q_k^2} \qquad \text{or } x_k + \frac{Q_{k-1}}{Q_k} \leqq 2\sqrt{2}. \tag{26}$$

From this, similarly to the proof of Borel's theorem, we obtain $x_{k+1} \leqq \sqrt{2}+1$, $Q_{k+1}/Q_k \leqq \sqrt{2}+1$ for $k \geqq v$, so that the sequence of quotients $a_{k+2}, a_{k+3}, \ldots$ consists only of two's and one's. Since x is not equivalent to $\frac{1}{2}(\sqrt{5}+1)$ this series must contain 2. Let $a_l = 2$ ($l \geqq k+2$); from $x_{l-1} = 2+1/x_l \leqq \sqrt{2}+1$ and $x_l \leqq \sqrt{2}+1$ we obtain $x_l = \sqrt{2}+1 = x_{l+1} = x_{l+2} = \ldots$. From (26) with $k \geqq l$ we find $Q_k/Q_{k+1} \leqq \sqrt{2}-1$, $Q_{k+1}/Q_k \geqq \sqrt{2}+1$ which combined with the earlier inequality $Q_{k+1}/Q_k \leqq \sqrt{2}+1$ gives an impossible result $Q_{k+1}/Q_k = \sqrt{2}+1$. The theorem is proved. Similarly to the above we may prove that for every number x_0 equivalent to $\sqrt{2}+1$, inequality $|x_0 - p/q| < 1/\varepsilon q^2$ is satisfied only by a finite number of p/q for every $\varepsilon > 2\sqrt{2}$.

This theorem together with Borel's theorem present the first two links in an infinite chain of similar theorems given by A. A. Markov in his remarkable work: 'On binary quadratic forms of a positive discriminant' [54] (see ch. IV and notes to ch. IV).

§ 7. Relative minima of the form $x-\omega y$

Let ω be a real irrational number. We say that a pair of integers p and $q > 0$ gives a *relative minimum* of a linear form $x-\omega y$, if the inequalities $|x-\omega y| \leqq |p-\omega q|, 0 \leqq y \leqq q$ are satisfied only by integers $x = p$, $y = q$ (not taking into account $x = 0$, $y = 0$). The problem of finding all the relative minima of a given linear form has led Lagrange to the discovery of important properties of convergents which is expressed in the following theorem.

THEOREM 10. *Let* $\omega = [a_1, a_2, \ldots]$ *be an irrational number, and let* $P_0/Q_0, P_1/Q_1, P_2/Q_2, \ldots$ *be its convergents. Then the pair of numbers* (P_1, Q_1) *with* $a_2 > 1$, *and all pairs* $(P_2, Q_2), (P_3, Q_3), \ldots$ *give relative minima of the form* $x-\omega y$, *and the form has no other relative minima.*

Let (P_k, Q_k) be one of the pairs, i.e. $k \geqq 2$ or $k = 1$ with $a_2 > 1$. Consider a pair of integers x, y satisfying inequalities

$$|x-\omega y| \leqq |P_k-\omega Q_k|, \qquad 0 \leqq y < Q_{k+1} \tag{27}$$

Defining integers m, n by conditions

$$x = mP_k+nP_{k+1}, \qquad y = mQ_k+nQ_{k+1}, \tag{28}$$

we have

$$x-\omega y = m(P_k-\omega Q_k)+n(P_{k+1}-\omega Q_{k+1}). \tag{29}$$

For m and n distinct from zero, we must have $mn > 0$, since $P_k-\omega Q_k$ and $P_{k+1}-\omega Q_{k+1}$ are of different sign, and for $mn < 0$, (29) contradicts (27). But for $mn > 0$, (28) contradicts (27). For $m = 0$, (27) and (28) give $n = 0$, i.e. $x = 0, y = 0$; for $m \neq 0$, $n = 0$ we find from (27) and (29) that $m = \pm 1$ and $x = P_k$, $y = Q_k$. Thus, inequalities (27) are satisfied only by a pair of numbers $x = P_k, y = Q_k$. Therefore, all pairs (P_k, Q_k) give relative minima of the form $x-\omega y$. Conversely, let $x = p, y = q > 0$ be a pair of numbers, giving a relative minimum of the form $x-\omega y$. Choose k to satisfy $Q_k \leqq q < Q_{k+1}$, then for

$a_2 > 1$ we have $k \geqq 1$ and for $a_2 = 1$ we have $k \geqq 2$. If the pair p, q does not coincide with P_k, Q_k then by inequality (27) we have $|p-\omega q| > |P_k-\omega Q_k|$, which contradicts the hypothesis that p, q give a relative minimum of the form $x-\omega y$. Thus, $p = P_k$, $q = Q_k$ and Lagrange's theorem is proved.

Theorem 10 is of especial importance due to the fact that the property of convergents described in it allows better generalization than other properties of convergents. Many works of Minkowski, Hermite, Voronoy and Zolotarev, which generalise in various directions the algorithm of continued fractions, are based on the property of convergents to give relative minima of the form $x-\omega y$.

§ 8. Arithmetical applications of Dirichlet's inequality

Theorem 8 (§ 1) has important arithmetical corollaries. Let p be a prime of the form $4n+1$ and let N be an integer, satisfying the congruence $N^2+1 \equiv 0 \pmod p$ (§ 8, ch. I). By theorem 8, we may select for number $\omega = N/p$ a fraction a/b such that $0 < b < \sqrt{p}$, $N/p = a/b+\theta/b\sqrt{p}$ where $|\theta| < 1$; for an integer $c = Nb-pa$ we have $|c| < \sqrt{p}$. Further, $c^2+b^2 \equiv b^2(N^2+1) \equiv 0 \pmod p$ and since $0 < c^2+b^2 < 2p$ we have $p = c^2+b^2$. Thus, *every prime of the form* $4n+1$ *is a sum of two squares*. Later we shall see that such a representation of a prime p is unique (apart from signs and the interchange of c and b). This theorem was stated by Fermat and first proved by Euler. In further chapters of this book we shall meet many various proofs of this theorem. The proof given here originates from Hermite (see [23], 'Note sur un théorème relative aux nombres entiers', p. 264).

Let $p > 2$ be a prime, and let e be a divisor of $p-1$ ($e \geqq 2$). It is known (§ 6, ch. I) that a reduced system of residues modulo p consists of $(p-1)/e$ residues of degree e modulo p, and of $(e-1)(p-1)/e$ nonresidues. Let N be a nonresidue of degree e. On finding a fraction a/b satisfying $0 < b < \sqrt{p}$, $|N/p-a/b| < 1/b\sqrt{p}$, two possibilities occur: 1) either b (which is greater than zero and less than $\sqrt{p}$) is a non-residue of degree e modulo p or 2) b is a residue and then $c = Nb-pa$ (whose absolute value is less than $\sqrt{p}$) is a non-residue.

Since the ratio of a non-residue and a residue is always a non-residue, this gives: 1) *the numbers* $-1, 1, 2, \ldots [\sqrt{p}]$ *always contain a non-residue of degree e to modulus p*. Therefore, 2) *between* $\sqrt{p}-1$ *and*

$2\sqrt{p}$ *there is always a non-residue of degree e to modulus p.* In fact, suppose all numbers $[\sqrt{p}]$, $[\sqrt{p}]+1, \ldots [2\sqrt{p}]$ are residues of degree e; then $2 = 2[\sqrt{p}]/[\sqrt{p}]$ is also a residue. If there exists a non-residue r between zero and $[\sqrt{p}]$ then all numbers $r, 2r, 2^2r, \ldots$ are non-residues; but among these numbers one lies within limits $\sqrt{p}, 2\sqrt{p}$ which contradicts the supposition. If all the numbers between 0 and $\sqrt{p}$ are residues, then, by 1 the number -1 is a non-residue of degree e. Take a circle of length p and let us represent all integers $-1, 0, 1, 2, \ldots$ by a sequence of equidistant points on this circle so that the numbers congruent modulo p fall on the same point on the circle. For $p = 3$ the proposition is obious. Taking $p > 3$ we have

$$[2\sqrt{p}] < p < ([2\sqrt{p}]-1)[\sqrt{p}].$$

Taking $s = [\sqrt{p}]$ consider the products $s, 2s, \ldots [2\sqrt{p}]s$ which, by our hypothesis are residues of degree e. Since $[2\sqrt{p}]s - s > p$, the points representing the products fill all the circle C and, consequently one of them falls into the interval $p-s, p$. In other words, there exists a number l such that $0 < l < s = [\sqrt{p}]$ and $p-l$ is a residue; l itself is then a non-residue of degree e. Thus, the supposition that proposition 2 is false leads to a contradiction in every case. 3) *The numbers* $m+1, m+2, \ldots, m+[2\sqrt{p}]$ *for every m contain a non-residue of degree e modulo p.* In fact, assuming that none of these numbers are divisible by p, and that they are residues of degree e, let us take by proposition 2, a non-residue r, where $[\sqrt{p}] \leqq r \leqq [2\sqrt{p}]$ and consider the products $(m+1)r, (m+2)r, \ldots, (m+[2\sqrt{p}])r$ which are non-residues. By the above inequalities, these points cover up all the circle C, and since they are at a distance r from each other, one of them falls into the interval $(m+1, m+[2\sqrt{p}])$ which contradicts the hypothesis. It is easy to conclude from propositions 1 and 2 that proposition 3 also holds when one of the numbers $m+1, m+2, \ldots m+[2\sqrt{p}]$ is divisible by p.

The reasonings concerning non-residues of degree e originate from I. M. Vinogradov.

In order to generalize Hermite's method, let us consider representations of an integer $m > 0$ by a form x^2+ay^2 where $a \neq 0$ is an integer, and a is not a proper square. Two representations x, y and x', y' are considered the same if and only if $x = x', y = y'$. If $(x, y) = 1$, the representation is called *proper*; from equation $x^2+ay^2 = m$ it is clear that for proper representations $(y, m) = 1$. Let x, y

be a proper representation of m; defining N from the congruence $x+Ny \equiv 0 \pmod{m}$ (which has a single solution, § 4, ch. I), we have $N^2y^2 \equiv x^2 \equiv -ay^2$ from which $N^2+a \equiv 0 \pmod{m}$. Thus, every proper representation x, y of a number m by a form x^2+ay^2 belongs to one definite root N of the congruence $N^2+a \equiv 0 \pmod{m}$. If two representations x, y and x', y' belong to the same root, then from congruences $x+Ny \equiv 0$, $x'+Ny' \equiv 0$ we find $xy'-x'y = mu$ (u is an integer), and the identity

$$(x^2+ay^2)(x'^2+ay'^2) = (xx'+ayy')^2+a(xy'-x'y)^2$$

shows that $xx'+ayy' = mt$, t – an integer. Numbers t, u satisfy the *Pellian equation*

$$t^2+au^2 = 1. \tag{30}$$

From the formulae obtained, we get

$$x' = tx-auy, \quad y' = ux+ty$$

or

$$x'+y'\sqrt{-a} = (x+y\sqrt{-a})(t+u\sqrt{-a}). \tag{31}$$

It is easy to see that, conversely, if t and u run through all the solutions of equation (30), then (31) gives all the representations x', y' (each occurring once) appertaining to the same root as x, y. For $a = 1$, equation (30) has four solutions: $t = \pm 1$, $u = 0$; $t = 0$, $u = \pm 1$ and the set of representations belonging to the same root consists of four pairs $(\varepsilon x, \varepsilon y)$, $(-\varepsilon y, \varepsilon x)$ where $\varepsilon = \pm 1$. For $a > 1$ equation (30) has two solutions $t = \pm 1$, $u = 0$ so that $(\varepsilon x, \varepsilon y)(\varepsilon = \pm 1)$ is the pair of representations belonging to the same root. Finally, when $-a > 0$ and is not a square, equation (30) has an infinite number of solutions. Let a be one of the numbers $1, \pm 2, \pm 3$, and let m be an integer, greater than 1, and relatively prime to $2a$. Take one of the roots of the congruence $N^2+a \equiv 0 \pmod{m}$ and assume in theorem 8

$$\omega = \frac{N}{m}, \quad \tau = \frac{\sqrt{m}}{\sqrt[4]{|a|}} > 1;$$

then we can find a fraction p/q for which

$$0 < q \leqq \frac{\sqrt{m}}{\sqrt[4]{|a|}}, \quad \left|\frac{N}{m} - \frac{P}{q}\right| < \frac{1}{\tau q}.$$

Taking $X = -Nq+mp$, $Y = q$ we may write

$$X^2+aY^2 \equiv q^2(N^2+a) \equiv 0 \pmod{m},$$
$$|X| < \sqrt{m}\sqrt[4]{|a|}, \quad 0 < Y \leqq \frac{\sqrt{m}}{\sqrt[4]{|a|}}.$$

Consequently, for $a > 0$ we have $0 < X^2+aY^2 < 2m\sqrt{a}$, for $a < 0$ we have $0 < |X^2+aY^2| < m\sqrt{|a|}$. Further $X+NY \equiv 0 \pmod{m}$. Take $X+aY^2 = \lambda m$; then from $((N^2+a)/m)q^2-2Npq+mp^2 = \lambda$ and from expressions for X, Y we see that the greatest common divisor of X, Y divides both λ and m. Thus, we can say: for every root N of congruence $N^2+a \equiv 0 \pmod{m}$, we may find integers X, Y such that

$$X^2+aY^2 = \lambda m, \quad X+NY \equiv 0 \pmod{m},$$
$$0 < \lambda < 2\sqrt{a} \quad \text{for } a > 0, \qquad 0 < |\lambda| < \sqrt{|a|} \quad \text{for } a < 0 \tag{32}$$

Moreover, the greatest common divisor of X, Y divides both λ and m. This result, together with the expression for the number of solutions of $N^2+a \equiv 0 \pmod{m}$ in § 9, ch. I, enables us to solve completely the problem of representation of numbers by a form x^2+ay^2, where the values of a are as above. Note, that for the existence of proper representations of m by a form x^2+ay^2 it is *necessary* that the congruence $N^2+a \equiv 0 \pmod{m}$ is solvable, i.e. that $-a$ is a quadratic residue of m.

1) $a = 1$. In (32) for every N we have $\lambda = 1$ and consequently numbers X and Y are relatively prime. If m is odd then for the existence of representations of m by the form x^2+y^2 it is necessary that every divisor of m is of the form $4n+1$, in which case there are $4 \cdot 2^{\nu}$ proper representations (ν is the number of distinct prime divisors of m, § 9, ch. I). The number of *all* representations of *any* odd m by a form x^2+y^2 is, clearly, represented by the sum $4\sum 2^{\nu}$ taken over all factorisations $m = d^2k$ with $d > 0$ selected in such a way that k consists exclusively of primes of the form $4n+1$. $\nu \geqq 0$ denotes the number of distinct prime divisors of k. Taking $m = p^{\alpha}p'^{\alpha'} \ldots$, where p, p', ... are distinct odd primes, we see that the sum $\sum 2^{\nu}$ is equal to the product of similar sums constructed for separate powers p^{α}, $p'^{\alpha'}$, ... It is easy to see that the value of the sum $\sum 2^{\nu}$ for number $p^{\alpha} = d^2k$ coincides in all cases with the sum $1+(-1/p)+(-1/p^2)+\ldots+(-1/p^{\alpha})$. Therefore, the number of all representations of m by a form x^2+y^2 is equal to $4\sum(-1\ d)$ where the summation is performed over all divisors of m.

It is easy to extend this result to the case of an even m. Let n be an arbitrary integer. Since in the equation $2n = x^2+y^2$ the numbers x, y are of the same parity, we can assume $x = x'+y'$, $y = x'-y'$ and find integers x', y' for which $n = x'^2+y'^2$. Thus, to every representation of 2n by a form x^2+y^2, there corresponds a representation of n by the same form, and conversely; denoting by $N(n = x^2+y^2)$ the number of all solutions of equation $n = x^2+y^2$ in integers x, y (considering two solutions x, y and x', y' the same only if $x = x'$, $y = y'$), we can write the above result as follows

$$N(2n = x^2+y^2) = N(n = x^2+y^2).$$

On the other hand, introducing an arithmetical function

$$\rho(n) = \sum \left(\frac{-1}{\delta}\right) = \sum (-1)^{\frac{1}{2}(\delta-1)}, \qquad n = d\delta, \quad \delta \text{ odd} \tag{33}$$

the above result may be formulated as follows: *the number of representations of an integer n by a form* x^2+y^2 *equals to four times the difference of the number of odd divisors of n of the form* $4k+1$ *and the number of odd divisors of n of the form* $4k+3$. *Symbolically*

$$N(n = x^2+y^2) = 4\rho(n). \tag{34}$$

If we agree that $\rho(0) = \frac{1}{4}$ then (34) is true even for $n = 0$. This result shows, in particular, that a prime of the form $4k+1$ may be represented as a sum of two squares in one way only, apart from the change of sign and interchange of x and y.

2) $a = 2$. In (32) $\lambda = 1$ or 2. Since (X, Y) divides both λ and m, and m is odd by supposition, X and Y are relatively prime. If $\lambda = 1$, then X, Y is a proper representation of m by the form x^2+2y^2 belonging to root N; if $\lambda = 2$, then, clearly, the proper representation is provided by numbers $-Y, \frac{1}{2}X$. Thus, if the congruence $N^2+2 \equiv 0 \pmod{m}$ is solvable (i.e. m consists exclusively of primes of forms $8k+1$ or $8k+3$) then, again, there exist proper representations of m, belonging to any root N. The number of all proper representations of m is equal to $2 \cdot 2^{\nu}$(§ 9, ch. I), where ν is the number of distinct prime factors of m. Therefore, similarly to the above, the number of all representations of an odd number m by a form x^2+2y^2 is equal to $2\sum(-2/d)$, where the summation is performed over all the divisors of m. Noting that

$N(2n = x^2+2y^2) = N(n = x^2+2y^2)$ and introducing an arithmetical function

$$\psi(n) = \sum\left(\frac{-2}{\delta}\right) = \sum(-1)^{(\delta^2-1)/8+(\delta-1)/2},$$

$$n = d\delta, \quad \delta \text{ odd}; \quad \psi(0) = \tfrac{1}{2} \qquad (35)$$

we obtain: *the number of representations of an integer n by a form* x^2+2y^2 *equals to twice the difference of the number of divisors of n of the form* $8k+1$ *or* $8k+3$ *and the number of divisors of n of the form* $8k+5$ *or* $8k+7$ i.e.

$$N(n = x^2+2y^2) = 2\psi(n), \qquad n \geqq 0. \qquad (36)$$

In particular, the Fermat-Euler theorem follows: *every prime of the form* $8n+1$ *or* $8n+3$ *is uniquely representable as a square plus twice a square.*

3) $a = 3$. In (32) $\lambda = 1, 2$ or 3 and, since $(m, 6) = 1$ we always have $(X, Y) = 1$. The value $\lambda = 2$ is impossible since for this value X and Y are of the same parity and $2m = X^2+3Y^2 \equiv 0 \pmod 4$. Numbers X, Y with $\lambda = 1$, and numbers $-Y, \frac{1}{3}X$ with $\lambda = 3$, give a proper representation belonging to the root N (if the congruence $N^2+3 \equiv 0 \pmod m$ is solvable). Therefore, the number of all representations of an odd number m not divisible by 3, by the form x^2+3y^2 is equal to $2\sum(-3\ d)$ where the sum is taken over all divisors d of m. Let n be a number, not divisible by 3. Consider equation $4n = x^2+3y^2$. For n even x, y are, clearly, even and

$$n = \left(\frac{x}{2}\right)^2+3\left(\frac{y}{2}\right)^2.$$

Therefore, if n is even $N(4n = x^2+3y^2) = N(n = x^2+3y^2)$. Let us denote the number of solutions of equation $n = x^2+3y^2$ whose variables satisfy some additional conditions by the same sign $N(n = x^2+3y^2)$ with the additional conditions written in brackets after the equation; thus for n odd

$$N(4n = x^2+3y^2) = N(n = x^2+3y^2)+N(4n = x^2+3y^2, x, y - \text{odd}) \qquad (37)$$

To determine the second term on the right hand side we use the identity $4(x'^2-3y'^2) = (x'-3y')^2+3(x'+y')^2$ by this identity, to

every solution of equation $n = x'^2+3y'^2$ there corresponds, by formulae $x = x'-3y'$, $y = x'+y'$ a solution x, y of equation $4n = x^2+3y^2$ in which x, y are odd and $x \equiv y \pmod 4$ (since n is odd). Conversely, to every solution of equation $4n = x^2+3y^2$ satisfying the conditions: x, y are odd, $x \equiv y \pmod 4$, there corresponds, by formulae $x' = \frac{1}{4}(x+3y)$, $y' = \frac{1}{4}(y-x)$ a solution of equation $n = x'^2+3y'^2$. Consequently

$$\begin{aligned} N(4n = x^2+3y^2, x, y - \text{odd}) &= 2N(4n = x^2+3y^2, x, y \text{ odd}, x \equiv y(4)) = \\ &= 2N(n = x^2+3y^2) \end{aligned}$$

and (37) gives for odd n

$$N(4n = x^2+3y^2) = 3N(n = x^2+3y^2)$$

The above exposition enables us to say that the number of representations of an integer n, not divisible by 3, by a form x^2+3y^2, is equal to zero if the greatest power of 2 dividing n is odd; if, however, $n = 2^\alpha m$ (α – even, > 0, m – odd), then the number of representations is equal to $6\sum(-3/d)$, where the summation is performed over all the divisors of m. Finally, noting that $N(3n = x^2+3y^2) = N(n = x^2+3y^2)$ we may state the following result: *the number of representations of an integer* $n = 2^\alpha m(\alpha \geqq 0, m - \text{odd})$ *by a form* x^2+3y^2 *is defined by the following* formulae

$$\begin{aligned} N(2^\alpha m = x^2+3y^2) &= 0 && \text{for } \alpha \text{ odd} \\ &= 6\chi(m) && \text{for } \alpha > 0 \text{ even} \\ &= 2\chi(m) && \text{for } \alpha = 0 \end{aligned} \tag{38}$$

where

$$\chi(m) = \sum\left(\frac{-3}{d}\right), \qquad m = d\delta, \quad (m \text{ odd}). \tag{39}$$

Moreover, the Jacobi symbol $(-3/d)$ is assumed to be zero if d is divisible by 3. In particular, we obtain Euler-Fermat theorem: *every prime of the form* $6k+1$ *is uniquely representable as a sum of a square and three times a square.*

The theorems proved above on the forms x^2+y^2, x^2+2y^2, x^2+3y^2 (see (34), (36), (38)) find important applications in chapter V in the study of representations of numbers by quadratic forms with greater number of variables.

4) $a = -2$. Taking $m > 0$, odd, we have in (32) $\lambda = \pm 1$ and $(X, Y) = 1$. If $\lambda = +1$, then X, Y give a solution of equation $m = X^2 - 2Y^2$ belonging to the root N of the congruence $N^2 - 2 \equiv 0 \pmod{m}$; if, however, $\lambda = -1$, then the solution, clearly, is provided by numbers $X+2Y$, $X+Y$. Thus, if the congruence $N^2 - 2 \equiv 0 \pmod{m}$ is solvable, there exist proper representations x, y belonging to *every* root of this congruence. All representations x', y' belonging to the same root, are obtained from one of them x, y using (31) with t, u running through all solutions of equation $t^2 - 2u^2 = 1$. Further (§ 12) we shall see that all solutions of the latter equation are obtained by separating the rational and irrational parts in expression

$$\pm(3+2\sqrt{2})^k$$

where k, independently of sign $\pm$, runs through all the values $0, \pm 1, +2, \ldots$; (31) then becomes

$$x'+y'\sqrt{2} = \pm(x+y\sqrt{2})(3+2\sqrt{2})^k, \qquad k = 0, \pm 1, \pm 2, \ldots. \tag{40}$$

Now consider all (proper and improper) representations of number m by the form $x^2 - 2y^2$. Let us collect into the same class the representations connected by formula (40). Then, similarly to the above, we find that the number of different *representation classes* is equal to $\sum(2/d)$ where the summation is performed over all divisors d of number m. In order to select one representative from every representation class, let us note that for $m = x^2 - 2y^2 > 0$ we have $|x| > |y\sqrt{2}|$ and hence, taking sign $\pm$ in the right hand side of (40), by condition $\pm x = |x|$, we have $\pm(x+y\sqrt{2}) > 0$ and $x' > 0$. Noting further that the logarithms of numbers $\pm(x+y\sqrt{2})(3+2\sqrt{2})^k$ form an arithmetical progression, we choose k (uniquely) by condition

$$\frac{\sqrt{m}}{1+\sqrt{2}} \leqq x'+y'\sqrt{2} < \sqrt{m}(1+\sqrt{2}).$$

Since $x'+y'\sqrt{2} > 0$, these inequalities are equivalent to the following

$$\frac{x'^2-2y'^2}{3+2\sqrt{2}} \leqq x'^2+2y'^2+2\sqrt{2}x'y' < (x'^2-2y'^2)(3+2\sqrt{2}),$$

which, on simplification, gives

$$(x'+y'\sqrt{2})(x'-2y') > 0, \quad (x'+y'\sqrt{2})(x'+2y') \geqq 0,$$

or

$$x'+2y' > 0, \quad x'-2y' > 0$$

(since x' is odd). Thus, in every representation class there exists one, and only one, representation satisfying two inequalities $x \pm 2y > 0$, and we obtain the following theorem: *the number of representations of an odd number $m > 0$ by the form x^2-2y^2 where x and y satisfy the conditions $x+2y > 0$, $x-2y > 0$, is equal to $\sum(2/d)$, where the summation is performed over all divisors of m,* or

$$N(m = x^2-2y^2, x \pm 2y > 0) = \sum_{m=d\delta} \left(\frac{2}{d}\right), \qquad m \text{ odd} > 0.$$

In particular, *a prime of the form $8k+1$ or $8k+7$ is representable as a difference of a square and a double square x^2-2y^2 (uniquely with side conditions $x > 2y > 0$).*

The latter theorem may be extended to the case of an even and a negative m and similar theorems may be formulated for $a = -3$.

§ 9. Symmetric continued fractions

A continued fraction $[a_1, a_2, \ldots, a_n]$ is called symmetric if the sequence of numbers $a_n, a_{n-1}, \ldots, a_1$ coincides with $a_1, a_2, \ldots, a_n$. Assuming $P_n/Q_n = [a_1, a_2, \ldots, a_n]$, we find by (12) $P_n/P_{n-1} = [a_n, a_{n-1}, \ldots, a_1]$ so that $Q_n = P_{n-1}$ for symmetric fraction. Conversely, if the latter condition is satisfied, the fraction is, clearly, symmetric. Using equality $P_nQ_{n-1}-P_{n-1}Q_n = (-1)^n$ it is easy to transform the condition $Q_n = P_{n-1}$ into the following: a number $P/Q[P > Q \geqq 1, (P, Q) = 1]$ is representable by a symmetric continued fraction if and only if $Q^2 \pm 1 \equiv 0 \pmod{P}$.

Consider a symmetric continued fraction $P_n/Q_n = [a_1, a_2, \ldots]$ $(a_1 \geqq 2)$ with n quotients. If n is odd and greater than 1, then the sequence of quotients of this fraction is of the form $a_1, a_2, \ldots, a_k, a_{k+1}, a_k, \ldots, a_1$. Taking $x_{k+1} = [a_k, \ldots, a_1] = P_k/P_{k-1}$ we have

$$\frac{P_n}{Q_n} = \frac{P_{k+1}x_{k+1}+P_k}{Q_{k+1}x_{k+1}+Q_k} = \frac{P_{k+1}P_k+P_kP_{k-1}}{Q_{k+1}P_k+Q_kP_{k-1}}$$

from which

$$P_n = P_{k+1}P_k+P_kP_{k-1}, \quad Q_n = Q_{k+1}P_k+Q_kP_{k-1}$$

(since the numbers $P_{k+1}P_k+P_kP_{k-1}$, $Q_{k+1}P_k+Q_kP_{k-1}$ are, clearly, relatively prime). From $P_n = P_k(P_{k+1}+P_{k-1})$ and since $P_{k+1} > P_k \geqq a_1 > 1$ it follows that P_n is a composite number. Thus, if a symmetric continued fraction whose number of quotients is odd, greater than one, and whose first element is greater than or equal to 2, is represented by an ordinary fraction, then its numerator is not a prime. Next, let the number n of quotients of the fraction P_n/Q_n be even; then the sequence of quotients is of the form $a_1, a_2, \ldots, a_k, a_k, a_{k-1}, \ldots, a_1$. Taking $x_k = [a_k, \ldots, a_1] = P_k/P_{k-1}$ we find

$$\frac{P_n}{Q_n} = \frac{P_k x_k + P_{k-1}}{Q_k x_k + Q_{k-1}} = \frac{P_k^2 + P_{k-1}^2}{Q_k P_k + Q_{k-1} P_{k-1}}$$

$$P_n = P_k^2 + P_{k-1}^2, \quad Q_n = P_k Q_k + P_{k-1} Q_{k-1}.$$

Thus, the numerator of a symmetric fraction with an even number of quotients is a sum of two squares. These results on symmetric continued fractions form a basis of a simple and elegant proof of the Fermat theorem on primes of the form $4n+1$ (§ 8), originated by H. J. S. Smith. Let $p = 4n+1$ be a prime. We develop the numbers

$$\alpha_1 = \frac{p}{2}, \quad \alpha_2 = \frac{p}{3}, \quad \ldots, \quad \alpha_{2n-1} = \frac{p}{2n} \tag{41}$$

into continued fractions in such a way that their last element is greater or equal to 2. Since all $\alpha_i > 2$, the first elements in all fractions are greater or equal to 2. Let $\alpha_i = [a_1, a_2, \ldots, a_k]$ be one of the continued fractions described above. Clearly, the fraction $[a_k, a_{k-1}, \ldots, a_1]$ is also equal to one of the numbers α_j, in fact, its numerator is equal to the numerator of the fraction, $[a_1, a_2, \ldots a_k]$ i.e. p. The denominator of the fraction $[a_k, a_{k-1}, \ldots a_1]$ is equal to the numerator P_{k-1} of the penultimate convergent to the fraction $[a_1, \ldots, a_k]$. From $a_1 \geqq 2$, $a_k \geqq 2$, $k \geqq 2$ we have $1 < P_{k-1} < \frac{1}{2}p$ and since $p = 4n+1$, P_{k-1} is one of the numbers $2, 3, \ldots, 2n$. Thus, the fraction $[a_k, \ldots, a_1]$ belongs to the set of numbers α_i together with $[a_1, \ldots, a_k]$. But, since the number of such fractions is odd, $2n-1$, they must contain a symmetric continued fraction $[b_1, \ldots, b_l] = \alpha_j = p/(j+1)$. Number l cannot be odd, since the numerator p is a prime; consequently, l is even and p is the sum of two squares. This proof does not assume the solvability of congruence $x^2+1 \equiv 0 \pmod{p}$.

§ 10. Development of a quadratic irrationality into a continued fraction

Euler has observed that when a quadratic irrationality, i.e. a root of quadratic equation, is developed into a continued fraction, then, starting from some place, the continued fraction becomes periodic. This fact has been proved by Lagrange and presents one of the most remarkable discoveries of this author in the number theory. In order to prove Lagrange's theorem, we start with formulae for development of a root of a quadratic equation into a continued fraction. Let

$$ax^2+2bx+c = 0 \tag{42}$$

be a quadratic equation, whose coefficients a, b, c are relatively prime integers and whose determinant $d = b^2-ac > 0$ is not a perfect square. The roots of this equation will be called the irrationalities of determinant d; each of them is of the form $(\alpha_0+\sqrt{d})\beta_0$ where $d = \alpha_0^2+\beta_0\beta_{-1}$ and α_0, β_0, β_{-1} are integers (equal to $-b$, a, $-c$ for one and b_1-a, c for the other root). Take one of these roots $x = (\alpha_0+\sqrt{d})/\beta_0$ and let us develop it into a continued fraction. To obtain the first partial quotient, we must find an integer $a_1 = [x]$, which may be achieved by means of the following formulae

$$\left[\frac{\alpha_0+\sqrt{d}}{\beta_0}\right] = \left[\frac{\alpha_0+\lambda}{\beta_0}\right] \qquad \text{for } \beta_0 > 0$$

$$= \left[\frac{\alpha_0+\lambda+1}{\beta_0}\right] \qquad \text{for } \beta_0 < 0,$$

where $\lambda = [\sqrt{d}]$.

These formulae can be easily proved. Take $x = [a_1, a_2, \ldots, a_n, x_n]$; since every complete quotient x_n is, clearly an irrationality of determinant d, we may assume $x_n = (\alpha_n+\sqrt{d})/\beta_n$ where α_n and β_n are integers. Substituting expressions for x_{n-1} and x_n into $x_{n-1} = a_n+1/x_n$, and separating rational and irrational parts, we find recurrence relations for successive evaluation of numbers α_n, β_n:

$$\begin{aligned} \alpha_n &= \beta_{n-1}a_n-\alpha_{n-1} \qquad n = 1, 2, 3, \ldots \\ d &= \alpha_n^2+\beta_n\beta_{n-1} \qquad n = 0, 1, 2, \ldots \end{aligned} \tag{43}$$

The latter expression can be replaced by the following

$$\beta_n = \beta_{n-2}-a_n(\alpha_n-\alpha_{n-1}) \qquad (n = 1, 2, \ldots)$$

Let P_n/Q_n be the n-th convergent to number x ($n \geqq 1$). Take H. J. St. Smith's formula (see (14)) $x_1 x_2 \ldots x_n = (-1)^n/(P_n - xQ_n)$. Writing it for conjugate numbers x_i', and multiplying the two formulae obtained, we find

$$x_1 x_1' \cdot x_2 x_2' \ldots x_n x_n' = \frac{1}{(P_n - xQ_n)(P_n - x'Q_n)}.$$

But $x_i x_i' = (\alpha_i + \sqrt{d})/\beta_i \cdot (\alpha_i - \sqrt{d})/\beta_i = -\beta_{i-1}/\beta_i$ (by (43))

$$(P_n - xQ_n)(P_n - x'Q_n) = \frac{1}{a}(aP_n^2 + 2bP_nQ_n + cQ_n^2),$$

from which, on simplifying, we obtain a very important formula

$$aP_n^2 + 2bP_nQ_n + cQ_n^2 = (-1)^n \varepsilon \cdot \beta_n \qquad n = 0, 1, 2, \ldots \qquad (44)$$

where $\varepsilon = +1$ if the root $x = (\alpha_0 + \sqrt{d})/\beta_0$ of equation(42), developed into a continued fraction, coincides with $(-b + \sqrt{d})/a$ and $\varepsilon = -1$ if $x = (-b - \sqrt{d})/a$.

An irrational number of determinant d will be called *reduced* if $(\alpha + \sqrt{d})/\beta > 1$ and its conjugate $(\alpha - \sqrt{d})/\beta$ is negative and of absolute value less than one. For reduced numbers

$$|\alpha + \sqrt{d}| > |-\alpha + \sqrt{d}|, \qquad \alpha > 0, \beta > 0, \quad \alpha < \sqrt{d},$$
$$\sqrt{d} - \alpha < \beta < \sqrt{d} + \alpha$$

and if γ denotes the integer $(d - \alpha^2)/\beta$, then $\sqrt{d} - \alpha < \gamma < \sqrt{d} + \alpha$. Conversely, if $0 < \sqrt{d} - \alpha < \beta < \sqrt{d} + \alpha$ then the number $(\alpha + \sqrt{d})/\beta$ is reduced. Inequalities $0 < \alpha < \sqrt{d}$, $0 < \beta < 2\sqrt{d}$ show that there exists only a finite number of reduced numbers for every discriminant d. If x is a reduced number, $a_1 = [x]$ and $x = a_1 + 1/x_1$, then x_1 is also a reduced number. In fact $x_1 > 1$, $a_1 \geqq 1$ and, passing to conjugate numbers, we have $x' = a_1 + 1/x_1'$, from which $-1 < x_1' < 0$. This shows that in a development of a reduced number into a continued fraction, all the complete quotients $x_1, x_2, \ldots$ also are reduced numbers. The same regularity is observed in the opposite direction: for a given reduced number x there exists one and only one integer a for which $x_{-1} = a + 1/x$ is a reduced number; namely, this occurs when $a = [-1/x']$. Let a reduced number x be developed into a continued fraction $x = [a_1, a_2, a_3, \ldots]$. Since all complete quotients $x_1, x_2, \ldots$ are reduced numbers of determinant d, whilst the number of the latter

is finite, it follows that for some numbers $n \geqq 0$ and $n+k > n$, we have $x_n = x_{n+k}$ and therefore $x_{n-1} = x_{n+k-1}$, $x_{n-2} = x_{n+k-2}, \ldots$, $x = x_k$ i.e. x occurs in the sequence of complete quotients. Denoting by k the smallest number greater than zero for which $x_k = x$ we see that the sequence of complete quotients presents an infinitely repeating group $x_1, x_2, \ldots, x_{k-1}$, and, respectively, the sequence of quotients $a_1, a_2, \ldots$ consists of infinitely repeating group of numbers $a_1, a_2, \ldots, a_k$ i.e. the continued fraction for x is *purely periodic* fraction with period $a_1, a_2, \ldots, a_k$. Such a fraction is denoted by symbol $[\overline{a_1, a_2, \ldots, a_k}]$.

Let $x = [a_1, a_2, a_3, \ldots]$ be a non-reduced irrationality; it is easy to see that for sufficiently large n the convergent x_n is a reduced number. In fact, for $n \geqq 1$, $x_n > 1$, expressing x_n in terms of x, we obtain

$$x_n = -\frac{Q_{n-1}x - P_{n-1}}{Q_n x - P_n}, \quad x_n' = -\frac{Q_{n-1}}{Q_n}\,\frac{x' - \dfrac{P_{n-1}}{Q_{n-1}}}{x' - \dfrac{P_n}{Q_n}}$$

$$x_n' + 1 = \frac{1}{Q_n}\left(Q_n - Q_{n-1} + \frac{(-1)^{n-1}}{Q_n\left(x' - \dfrac{P_n}{Q_n}\right)}\right).$$

For a sufficiently large n, the differences $x' - P_{n-1}/Q_{n-1}$ and $x' - P_n/Q_n$ are arbitrarily near to $x' - x \neq 0$ and thus they are both of the same sign, whilst the expression $Q_n(x' - P_n/Q_n)$ is arbitrarily large in absolute value; therefore, by the above formulae, we have $x_n' < 0$, $x_n' + 1 > 0$ i.e. x_n is a reduced number. Denoting $x_n = [\overline{a_{n+1}, a_{n+2}, \ldots, a_{n+k}}]$ we obtain for x a *composite periodic fraction*

$$x = [\overline{a_1, \ldots, a_n, a_{n+1}, \ldots, a_{n+k}}]$$

Thus we arrive at Lagrange's theorem

THEOREM 11. *Every real quadratic irrationality develops into a periodic continued fraction.*

Conversely, it may be easily shown that a periodic continued fraction represents a quadratic irrationality; moreover, the value of a *purely periodic* fraction is always equal to a reduced number (Per-

ron [69], p. 80). Among the available proofs of Lagrange's theorem, the simplest one seems to be by Charves (Perron [69], p. 77).

§ 11. Inverse numbers

Let $x = (\alpha+\sqrt{d})/\beta$ be a quadratic irrationality of determinant $d = \alpha^2+\beta\gamma$. The number $\xi = (\alpha+\sqrt{d})/\gamma = -1/x'$ (of the same determinant) will be called inverse to α. If x is a reduced number, then, clearly, so is ξ. In this case the periods of continued fractions x and ξ are connected by a simple relationship, indicated by Galois. Namely, *the period of fraction ξ consists of numbers of period x written in the opposite order.* Let x_1 be the first complete quotient to x, so that $x = a_1+1/x_1$; then between their united numbers ξ, ξ_1 there exists a relationship $\xi_1 = a_1+1/\xi$, so that ξ is the first complete quotient to ξ_1. If $x = [a_1, a_2, \ldots, a_n]$ then, according to relationships between the convergents $x, x_1, \ldots, x_{n-1}$

$$x = a_1+\frac{1}{x_1}, \quad x_1 = a_2+\frac{1}{x_2}, \ \ldots, \ x_{n-1} = a_n+\frac{1}{x},$$

we have the following relationships between their united numbers $\xi, \xi_1, \ldots, \xi_{n-1}$:

$$\xi = a_n+\frac{1}{\xi_{n-1}}, \quad \xi_{n-1} = a_{n-1}+\frac{1}{\xi_{n-2}}, \ \ldots, \ \xi_1 = a_1+\frac{1}{\xi}$$

i.e. $\xi = \overline{[a_n, a_{n-1}, \ldots, a_1]}$ which is the Galois theorem.

Let $A = m/n > 1$ be a rational number, not a square. Taking $\lambda = [\sqrt{A}] \geqq 1$, we see that $x = \lambda+\sqrt{A}$ is a reduced number. Clearly, the first element of the continued fraction for x is 2λ; denote $x = \overline{[2\lambda, \lambda_1, \lambda_2, \ldots \lambda_k]}$ and let us prove that the sequence of numbers $\lambda_1, \lambda_2, \ldots, \lambda_k$ is symmetric, i.e. that it coincides with the sequence $\lambda_k, \lambda_{k-1}, \ldots, \lambda_1$. In fact, $\overline{[\lambda_1, \lambda_2, \ldots, \lambda_k, 2\lambda]} = 1/(x-2\lambda)$ $= 1/(\sqrt{A}-\lambda)$. By Galois theorem, for a number inverse to x we have

$$\frac{1}{\sqrt{A}-\lambda} = \overline{[\lambda_k, \lambda_{k-1}, \ldots, \lambda_1, 2\lambda]}$$

Comparing the two developments of $1/(\sqrt{A}-\lambda)$, we obtain the desired result. Thus, a continued fraction for a square root of a rational

number $\sqrt{A} = \sqrt{m/n}$ is of the form

$$\sqrt{A} = [\lambda, \overline{\lambda_1, \lambda_2, \ldots, \lambda_k, 2\lambda}], \qquad \lambda_k = \lambda_1, \quad \lambda_{k-1} = \lambda_2, \ldots \tag{45}$$

Symmetric part of period $\lambda_1, \lambda_2, \ldots, \lambda_k$ may be absent (for $A = \lambda^2+1$). A continued fraction of the form (45) is characteristic for a square root of a rational number. In other words, for an arbitrary $\lambda \geqq 1$, and an arbitrary symmetric sequence of numbers $\lambda_1, \lambda_2, \ldots, \lambda_k$, the square of the fraction $[\lambda, \overline{\lambda_1, \ldots, \lambda_k, 2\lambda}]$ is equal to a rational number. In fact, denoting by x the value of this fraction, we find that $x+\lambda$ is a purely periodic fraction and therefore (§ 10) $x+\lambda$ is a reduced number, from which, by Galois theorem, we have $1/(x'+\lambda) = [\overline{\lambda_k, \lambda_{k-1}, \ldots, \lambda_1, 2\lambda}]$. Comparing this with $1/(x-\lambda) = [\overline{\lambda_1, \ldots, \lambda_k, 2\lambda}]$, we obtain $x' = -x$ i.e. x^2 is equal to a rational number.

Consider another property of a continued fraction of a square root of an *integer* $A = d$. Let $\lambda = [\sqrt{d}]$ and let $\sqrt{d} = [\overline{\lambda, \lambda_1, \ldots, \lambda_k, 2\lambda}]$. The sequence of complete quotients $x = \sqrt{d}, x_1, x_2, \ldots$ is periodic, beginning with the second term, of period

$$x_1 = \frac{\alpha_1+\sqrt{d}}{\beta_1}, \quad x_2 = \frac{\alpha_2+\sqrt{d}}{\beta_2}, \ldots, x_{k+1} = \frac{\alpha_{k+1}+\sqrt{d}}{\beta_{k+1}} \tag{46}$$

The last number of this sequence is $x_{k+1} = [\overline{2\lambda, \lambda_1, \ldots, \lambda_k}] = \lambda+\sqrt{d}$. consequently, $\beta_{k+1} = 1$. Clearly, x_{k+1} is the only complete quotient in the sequence (46) whose denominator is 1. In fact, if for $1 \leqq i < k+1$ we have $\beta_i = 1$, then since $x_i = \alpha_i+\sqrt{d}$ is a reduced number, we have $\alpha_i < \sqrt{d} < \alpha_i+1$, $\alpha_i = \lambda$, $x_i = x_{k+1}$ from which $x_1 = x_{k-i+2}$ which is impossible for the shortest period (46).

Further study of the questions referred to in the present section may be found in the book by Perron [69] (ch. III).

§ 12. Pellian equation

Using the method of continued fractions as a base, Lagrange gave a method for solving in integers x, y a general equation of second degree

$$ax^2+2bxy+cy^2+2dx+2ey+f = 0$$

with integer coefficients. We do not give a detailed account of Lagrange's method here, since a similar method follows from Gauss's theory of quadratic forms (ch. IV); we demonstrate Lagrange's reasonings using as example an important *Pellian equation*

$$x^2 - dy^2 = \pm 1 \tag{47}$$

in which d is a given positive integer, not a square. If equation (47) has a solution $x > 0$, $y > 0$, then

$$\left| \frac{x}{y} - \sqrt{d} \right| = \frac{1}{\left(\frac{x}{y} + \sqrt{d} \right) y^2} < \frac{1}{2\sqrt{d-1}\, y^2} \leqq \frac{1}{2y^2}$$

and, consequently, the irreducible fraction x/y is a convergent to the continued fraction for $\sqrt{d}$ (§ 5). Thus, solution of equation (47) in positive x, y must be found among the numerators and denominators of convergents to $\sqrt{d}$. Let (§ 11) $\sqrt{d} = [\lambda, \overline{a_1, a_2, \ldots, a_k}]$ where $\lambda = [\sqrt{d}]$, $a_k = 2\lambda$; take a sequence of complete quotients of this fraction: $x = \sqrt{d}$, $x_i = (\alpha_i + \sqrt{d})/\beta_i$ $(i = 1, 2, 3, \ldots)$. Remembering formula (44), we have for the ith convergent P_i/Q_i of fraction $\sqrt{d} = [\lambda, a_1, a_2, \ldots]$ the following formula

$$P_i^2 - dQ_i^2 = (-1)^i \beta_i \qquad (i = 1, 2, 3, \ldots).$$

This formula shows that those and only those convergents P_i/Q_i are solutions of (47) for which denominator β_i in the corresponding complete quotient x_i is equal to 1. But the sequence of complete quotients $x_1, x_2, \ldots$ is a recurrent sequence with period $x_1, x_2, \ldots, x_k$ and we saw in § 4 that in this period only one complete quotient has denominator 1, namely x_k. Therefore, the solutions of (47) in positive x, y are exhausted by numbers $x = P_{ik}$, $y = Q_{ik}$ $(i = 1, 2, 3, \ldots)$. Moreover, clearly, equation $x^2 - dy^2 = +1$ always has solutions, whilst equation $x^2 - dy^2 = -1$ has solutions only for odd k. All solutions of (47) thus obtained are connected by a simple relationship. Take $P_k = T$, $Q_k = U$. Obviously, it is the solution of (47) in *least* positive numbers. By S. Smith's formula (14), we have

$$x_1 x_2 \ldots x_k = \frac{(-1)^k}{P_k - Q_k\sqrt{d}} = \frac{(-1)^k}{T - U\sqrt{d}}$$

$$x_1 x_2 \ldots x_{ik} = \frac{(-1)^{ik}}{P_{ik} - Q_{ik}\sqrt{d}}, \qquad i = 1, 2, 3, \ldots.$$

But, since the sequence of complete quotients is periodic, we have $x_1 x_2 \dots x_{ik} = (x_1 x_2 \dots x_k)^i$ from which

$$P_{ik} + Q_{ik}\sqrt{d} = (T + U\sqrt{d})^i, \qquad i = 1, 2, 3, \dots .$$

Finally noting that solutions x, y of equation (47) satisfy $x - y\sqrt{d} = \pm(x + y\sqrt{d})^{-1}$, we may state the following theorem, which is a summary of a complete solution of a Pellian equation.

THEOREM 12. *Let d be positive and not a square. Developing $\sqrt{d}$ into a continued fraction, we find its first (shortest) period; let it end with the term a_k. Discarding all partial quotients of the continued fraction which are after a_k, we obtain the convergent whose numerator and denominator provide the smallest solution $x = T$, $y = U$ of equation $x^2 - dy^2 = \pm 1$. The remaining solutions are found from*

$$x + y\sqrt{d} = \pm(T + U\sqrt{d})^n, \qquad n = 0, \pm 1, \pm 2, \dots \tag{48}$$

Moreover, equation $x^2 - dy^2 = -1$ is solvable if and only if the period of the continued fraction for $\sqrt{d}$ consists of an odd number of terms, in which case all its solutions are obtained from (48) with odd index $n = \pm 1, \pm 3, \dots$. Equation $x^2 - dy^2 = +1$ always has an infinite number of solutions. They may be obtained from (48) with any integer n if k (the number of terms of the period of the fraction $\sqrt{d}$) is even, and for every even integer n if k is odd.

In the German translation of Legendre's book 'Essai sur la théorie des nombres' (see [40]), there is a table of the smallest solutions T, U of equation $x^2 - dy^2$ for all integers d up to 1000. Numbers T, U change with increase of d quite irregularly, from small values to quite large ones. For example, for $d = 60$, we have $T = 31$, $U = 4$, and for $d = 61$ we have $T = 29718$, $U = 3805$.

For equation $x^2 - dy^2 = -1$ we find that until now there exists no other method of solving it, apart from developing $\sqrt{d}$ into a continued fraction. Dirichlet (see [13] vol. I p. 221) has indicated some particular values of d for which equation $x^2 + dy^2 = -1$ is solvable. Of Dirichlet's theorems the following is of most importance: *for a prime p of form $4n+1$ equation $x^2 - py^2 = -1$ is always solvable.* In fact, let $T > 0$, $U > 0$ be the smallest solution of equation

$$x^2 - py^2 = +1$$

It follows from $T^2-pU^2 = 1$ that U is even; writing this equation in the form $\frac{1}{2}(T+1)\cdot\frac{1}{2}(T-1) = p(\frac{1}{2}U)^2$ and noting that $\frac{1}{2}(T+1)$, $\frac{1}{2}(T-1)$ are positive, relatively prime integers, we find, for some sign $\varepsilon = \pm 1$: $\frac{1}{2}(T+\varepsilon) = t^2$, $\frac{1}{2}(T-\varepsilon) = pu^2$, where t, u are integers, greater than zero, satisfying $2tu = U$. If $\varepsilon = +1$, then

$$t^2-pu^2 = +1,$$

which is impossible, since $0 < u \leqq \frac{1}{2}U$; consequently, $\varepsilon = -1$ and

$$t^2-pu^2 = -1.$$

Moreover, it is clear that t, u is the least solution of this equation. Applying a similar reasoning to equation $t^2-pu^2 = 1$ with a prime p of the form $4n+3$ we obtain the following theorem: *for a prime p of the form $4n+3$ equation $x^2-py^2 = \pm 2$ is always solvable for one (and only one) sign $\pm$*. The sign $\pm$ in the above equation does, obviously, coincide with $(2/p)$.

§ 13. Johann Bernoulli's question

Johann Bernoulli (the astronomer, and the grandson of mathematician Bernoulli) in his collected astronomical papers 'Recueil pour les astronomes' (1772) indicates some interesting rules for evaluating the table of *proportional parts*. The problem consists in finding the nearest integers to a sequence of multiples of a given number ξ. The integer nearest to x (i.e. integer a defined by inequalities $-\frac{1}{2} \leqq x - a < +\frac{1}{2}$) is equal to $[x+\frac{1}{2}]$; Therefore, the question is reduced to the composition of a sequence of numbers $[m\xi+\frac{1}{2}]$, $(m = 1, 2, 3, \ldots)$. Clearly, when m is increased by one, then $[m\xi+\frac{1}{2}]$ is increased either by $[\xi]$ or by $[\xi]+1$. If we have a rule showing when we should add $[\xi]$, and when $[\xi]+1$, the quantities

$$[m\xi+\tfrac{1}{2}] \qquad (m = 1, 2, \ldots)$$

can be formed by means of additions only. J. Bernoulli gives these rules (without proof), which are based on the development of ξ into a continued fraction. The proof of Bernoulli's rules and further extensions are given in the article by A. A. Markov, the contents of which we give here, restricting ourselves to the case of an *irrational* ξ.

Let us set out to construct for a given irrational number ξ a sequence of numbers $[m\xi]$ $(m = 1, 2, 3, \ldots)$. Without loss of generality we may assume $0 < \xi < 1$; then $[(m+1)\xi]-[m\xi] = g_m$ is either

equal to zero, or to one. Christoffel called the sequence $g_1 g_2 g_3 \ldots$ formed of zeros and ones, the *characteristic of number* ξ. If the characteristic of ξ is known, then the construction of numbers $[m\xi]$ can be performed by means of additions only. Obviously, the characteristic of a number ξ determines this number completely. For future reasons, the characteristic may also be written in another form, replacing numbers 0 and 1 by letters c and d, so that the sequence $g_1 g_2 g_3 \ldots$ is replaced by some sequence of letters c and d. In some portion of this sequence letter c occurs k times in succession, after it letter d occurs l times, and then letter c occurs n times in succession, etc. this will be abbreviated as follows: $c^k d^l c^n \ldots$. Let $\xi = 1/(s+\xi_1)$ where s is an integer > 0 and $0 < \xi_1 < 1$. For every integer $k \geqq 1$

$$(ks+[k\xi_1])\xi = k-\xi \cdot \{k\xi_1\}, \quad (ks+[k\xi_1]+1)\xi = k+\xi(1-\{k\xi_1\}),$$

where $\{x\}$ denotes the *fractional part* of number x, i.e. the difference $x-[x]$. Taking $ks+[k\xi_1] = \alpha_k (k = 1, 2, 3, \ldots)$ and noting that $0 < \xi < 1$, $0 < \{k\xi_1\} < 1$, we find $[\alpha_k \xi] = k-1$, $[(\alpha_k+1)\xi] = k$ from which

$$[\alpha_{k+1}\xi]-[(\alpha_k+1)\xi] = g_{\alpha_k+1}+g_{\alpha_k+2}+\ldots+g_{\alpha_{k+1}-1} = 0,$$

$$g_{\alpha_k+1} = g_{\alpha_k+2} = \ldots = g_{\alpha_{k+1}-1} = 0$$

and

$$[(\alpha_{k+1}+1)\xi]-[\alpha_{k+1}\xi] = g_{\alpha_{k+1}} = 1;$$

thus, in the characteristic of number ξ we select a group of terms $g_{\alpha_k+1}, g_{\alpha_k+2}, \ldots g_{\alpha_{k+1}}$, which may be represented as follows, $c^{\alpha_{k+1}-\alpha_k-1}d$. Noting that if $k = 1$, then $\alpha_k = s$, we have, beginning with term g_{s+1}, the following composition of the characteristic: $c^{\alpha_2-\alpha_1-1}dc^{\alpha_3-\alpha_2-1}dc^{\alpha_4-\alpha_3-1}$. The group of terms $g_1 g_2 \ldots g_s$, as we can see from equalities $[s\xi] = 0$, $[(s+1)\xi] = 1$, is of the form $c^{s-1}d$. Let $h_1 h_2 h_3 \ldots$ be the characteristic of ξ_1 written by means of zeros and ones, so that $h_i = [(i+1)\xi_1]-[i\xi_1]$. Then $\alpha_{k+1}-\alpha_k = s+h_k$ and the characteristic of ξ is represented as follows $c^{s-1}dc^{s-1+h_1}dc^{s-1+h_2}d \ldots$. Therefore, there exists the following connection between the characteristics of numbers ξ and ξ_1: the characteristic of ξ is obtained from the characteristic of ξ_1 by replacing in the latter every c by group $c_1 = c^{s-1}d$, every d by group $d_1 = c^s d$, and adjoining group c_1 on the left. Denote by $\chi(c, d)$ and $\chi_1(c, d)$ the characteristics of ξ and ξ_1 respectively. The rule can then be visually demonstrated as follows:

$\chi(c, d) = c_1 \chi_1(c_1, d_1)$, Further, let $\xi_1 = 1/(s_1 + \xi_2)$, where s_1 is an integer > 0 and $0 < \xi_2 < 1$. Denoting by $\chi_2(c, d)$ the characteristic of ξ_2 we find from the above $\chi_1(c, d) = c_1' \chi_2(c_1', d_1')$ where $c_1' = c^{s_1 - 1} d$ and $d_1' = c^{s_1} d$. The groups c_1', d_1' on replacing of c and d by groups $c_1 = c^{s-1} d$ and $d_1 = c^s d$, transform into groups $c_2 = c^{s_1 - 1} d_1$ and $d_2 = c^{s_1} d_1$ and we obtain $\chi(c, d) = c_1 c_2 \chi_2(c_2, d_2)$. Continuing in a similar manner, we obtain the following rule for composition of the characteristic of number ξ: *let ξ be an irrational number, lying between zero and one, and let $\xi = [0, s, s_1, s_2, \ldots]$ be its development into a continued fraction; we construct*, successively, groups

$$\left.\begin{array}{llll} c_1 = c^{s-1} d, & c_2 = c_1^{s_1 - 1} d_1, & c_3 = c_2^{s_2 - 1} d_2, & \ldots, \\ d_1 = c^s d, & d_2 = c_1^{s_1} d_1, & d_3 = c_2^{s_2} d_2, & \ldots, \end{array}\right\} \tag{49}$$

Then the characteristic of ξ is represented by a sequence $c_1 c_2 c_3 c_4 \ldots$.

For example, for $\xi = \sqrt{2} - 1 = [0, 2, 2, 2, \ldots]$ groups (49) are

$$\begin{array}{lll} c_1 = cd, & c_2 = cdc^2 d, & c_3 = cdc^2 dcdcdc^2 d, \ldots, \\ d_1 = c^2 d, & d_2 = cdcdc^2 d, & d_3 = cdc^2 dcdc^2 dcdcdc^2 d, \ldots, \end{array}$$

so that the characteristic of ξ is $cdcdccdcdccdcdcdccd, \ldots$, which gives the following table

m: 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17. 18, 19, 20

$[m\xi]$: 0, 0, 1, 1, 2, 2, 2, 3, 3, 4, 4, 4, 5, 5, 6, 6, 7, 7, 7, 8, . . .,

Consider J. Bernoulli's question. Let $[(m+1)\xi + \frac{1}{2}] - [m\xi + \frac{1}{2}] = g_m$ for an irrational ξ lying between 0 and 1, and let us call the sequence $g_1 g_2 g_3 \ldots$, composed of zeros and ones, (similar to the characteristic), a *Bernoulli sequence*. Similarly to above, Bernoulli sequence will be written as a sequence of letters c and d. It follows from the identity $[m\xi + \frac{1}{2}] + [m(1-\xi) + \frac{1}{2}] = m$ $(m = 1, 2, 3, \ldots)$ that the Bernoulli sequence for numbers ξ and $1 - \xi$ satisfy a very simple relationship; namely, the letters c, d of the first sequence correspond to the letters d, c, respectively, of the second sequence. Therefore, we may assume $0 < \xi < \frac{1}{2}$. Let $2\xi = 1/(s + \xi_1)$ where s is an integer > 0, $0 < \xi_1 < 1$ and let $\alpha_{2m-1} = (2m-1)s + [(2m-1)\xi_1]$ $(m = 1, 2, 3, \ldots)$. Then from $\alpha_{2m-1}\xi + \frac{1}{2} = m - \xi \cdot \{(2m-1)\xi_1\}$ we find, similarly to the above

$$[\alpha_{2m-1}\xi + \tfrac{1}{2}] = m - 1 \quad \text{and} \quad [(\alpha_{2m-1} + 1)\xi + \tfrac{1}{2}] = m,$$

from which it is evident that a part of Bernoulli sequence $g_{\alpha_{2m-1}+1} g_{\alpha_{2m-1}+2} \cdots g_{\alpha_{2m+1}}$ has the composition $c^{\alpha_{2m+1}-\alpha_{2m-1}-1}d$. Denoting the characteristic of ξ_1, written by means of zeros and ones, by $h_1 h_2 h_3 \ldots$, and noting that $\alpha_1 = s$, $[s\xi+\frac{1}{2}] = g_1+g_2+\ldots+g_{s-1} = 0$, $[(s+1)\xi+\frac{1}{2}] = g_1+\ldots+g_s = 1$, we obtain the following composition of the Bernoulli sequence for number ξ: $c^{s-1}dc^{2s-1+h_1+h_2} dc^{2s-1+h_3+h_4}d \ldots$. This yields the following rule for the composition of Bernoulli's sequence: *Let ξ be an irrational number, lying between 0 and $\frac{1}{2}$. We construct the characteristic of $\xi_1 = \{\frac{1}{2}\xi\}$ by the rule given above, and then split the elements of this characteristic into groups, each containing two elements. Every such group is then replaced by the following: a group of form cc is replaced by $c^{2s-1}d$, a group of the form cd or dc is replaced by $c^{2s}d$, a group of the form dd is replaced by $c^{2s+1}d$ (s denotes integer $[\frac{1}{2}\xi]$). Then adjoin $c^{s-1}d$ on the left of the sequence thus obtained. The resulting sequence of letters c and d is, the Bernoulli sequence for number ξ.* For example, for $\xi = 1/\sqrt{8}$ we have $\xi_1 = \sqrt{2}-1$, $s = 1$ and from the previous example we find for ξ the Bernoulli series *dccdccdcdccdccdccdccdccdcd* ..., which gives the following table

m: 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, ...

$[m\xi+\frac{1}{2}]$: 0, 1, 1, 1, 2, 2, 2, 3, 3, 4, 4, 4, 5, 5, 5, 6, 6, 6, 7, 7, 7, 8, 8, 8, 9, ...

Notes to chapter 2

§ 1. The theorem on Farey series which has been proved in this section is due to Cauchy (see K. Th. Vahlen [84]). Hurwitz [27] applied the Farey series to reduce binary quadratic forms of a positive and a negative determinant (see § 3, ch. II, and ch. IV).

§ 4. Numerators and denominators of convergents are examples of *recurrent* series, i.e. such series of numbers, whose general term satisfies a linear difference equation. The case of the equation of the second order with constant coefficients has been studied by Lucas [53]. The simplest of these series is the Fibonacci series:

$u_0 = 0$, $u_1 = 1$, $u_2 = 1$, $u_3 = 2$, $u_4 = 3$, $u_5 = 5$, $u_6 = 8$, $u_7 = 13, \ldots$

each term of which is equal to the sum of two preceding ones. This series (whose terms are nothing else but the denominators of convergents to a continued fraction $\frac{1}{2}(\sqrt{5}+1) = [1, 1, 1, \ldots]$ has many interesting properties (see Lucas [53], ch. XVIII), of which the following are of note: 1) the product of k consecutive terms of this series is divisible by $u_1 u_2 \ldots u_k$. 2) for m divisible by n, u_m is divisible by u_n.

Such properties of recurrent series simplify, in some cases, decomposition of large numbers into prime factors (see Bachmann [4], Lehmer [45]). Many mathematicians were interested in the question whether the Fibonacci series contains an infinite number of primes or not; but this problem is still unsolved.

Simple continued fractions given in the text correspond (for rational numbers) to the Euclidean Algorithm in which the remainders are always taken with + sign (§ 1, ch. I). If one performs successive divisions taking the remainders with $\pm$ sign, the continued fraction obtained is of the form

$$a_1 \pm \cfrac{1}{a_2 \pm \cfrac{1}{a_3 \pm \ddots}} ;$$

development of a rational number into such continued fractions has been studied in detail by Vahlen [84]. Development of irrational number into fractions of the form

$$a_1 - \cfrac{1}{a_2 - \cfrac{1}{a_3 - \ddots}}$$

has been studied by Hurwitz [25]. Finally, in the memoir 'Über die Entwicklung complexer Grössen in Kettenbrüche' [24] Hurwitz gives an interesting study of the development of a number into a continued fraction $a_1 + 1/a_2 + \ldots$ with complex $a_1, a_2, a_3, \ldots$ of the form $m + n\varepsilon$ (m, n rational integers, ε – 3rd or 4th roots of unity).

§ 7. In the memoir 'On one question of arithmetic', P. L. Chebychev (see [81], pp. 639–684) solved a more general problem of defining the relative minima of a *linear function* $x - \omega y - \zeta$ (where ω, ζ are given real numbers). Chebychev obtained the following result: *there exists an infinite number of pairs of integers* x, y *satisfying the inequality*

$|x-\omega y-\zeta| < \varepsilon/|y|$ *where* $\varepsilon = \frac{1}{2}$. Chebychev's result has been improved by Minkowski [59], who has shown that the constant ε may be taken to be equal to $\frac{1}{4}$, and it cannot be made any smaller.

§ 8. Dirichlet himself (see Dirichlet [14], § 142) applied theorem 8 to the solution of the Pellian equation $x^2-dy^2 = 1$ (see § 12, ch. II).

In the VIth volume of 'Gesammelte Werke' by Jacobi [31] are given the tables of representation of primes $\leqq 11321$ by the form x^2+y^2, of primes $\leqq 12007$ by the form x^2+3y^2 and primes $\leqq 5953$ by the form x^2+2y^2. As it has been mentioned in the text, primes of the form $4n+1$, $6n+1$ and $8n+1$ or $8n+3$ are representable uniquely in the form x^2+y^2, x^2+3y^2, x^2+2y^2. It follows from (34), (36), (38) that if there exists a *proper* representation of a composite number by any of the forms x^2+y^2, x^2+3y^2, x^2+2y^2 then this representation is not unique. Euler used this fact to find whether a large number is a prime or a composite number. (See [17], vol. I, p. 379, vol. II pp. 198, 220, 249, 261, 270). If, for example, a number N has a proper representation $N = a^2+b^2$ $(a > b > 0)$ then to find the other representations we must test for which $x = 1, 2, 3, \ldots [\sqrt{\frac{1}{2}N}]$ the expression $N-x^2$ is a square. If there are no such x, apart from $x = b$, then N is a prime. If, however, we find another representation $N = a'^2+b'^2$ distinct from $N = a^2+b^2$ then N is a composite number, and, using numbers a, b, a', b' it is easy to construct a divisor of N. (See Euler [17], vol. I. p. 379). Moreover, in every particular case the number of trials may be diminished considerably. In his attempt to obtain a more efficient method for solving the problem, Euler considers the values of the product mn ($m > 0$, $n > 0$ relatively prime integers) for which the form mx^2+ny^2 represents every prime in no more than one way, but does not represent any composite number uniquely. Clearly, with these conditions, the form mx^2+ny^2 may also serve for recognising the prime numbers, and the number of necessary trials is less if the numbers m and n are greater. Such products mn Euler called *idoneal* numbers (numeri idonei), and he devoted a great amount of effort and time to find them. He succeeded in finding 65 idoneal numbers: 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12, 13, 15, 16, 18, 21, 22, 24, 25, 28, 30, 33, 37, 40, 42, 45, 48, 57, 58, 60, 70, 72, 78, 85, 88, 93, 102, 105, 112, 120, 130, 133, 165, 168, 177, 190, 210, 232, 240, 253, 273, 280, 312, 330, 345, 357, 385, 408, 462, 520, 760, 840, 1320, 1365, 1848.

The greatest idoneal number 1848 enabled Euler to establish

the primarity of many numbers (e.g. $18518809 = 197^2 + 1848 \cdot 100^2$), Euler did not succeed in finding any other idoneal numbers, in spite of the fact that he tried all numbers up to 10000. In 1901 Cunningham and Culler continued Euler's calculations up to 101200 and still could not find any idoneal numbers (see Frobenius [18]). Gauss has shown a close connection of these numbers with the theory of the genus of quadratic forms (D. A. [20], art. 303, see § 1, ch. VI). However this theory also does not help to discover any of the essential properties if idoneal numbers, and the question whether there are any more idoneal numbers apart from those found by Euler is still open. *

§ 10. An attempt to generalise periodic continued fractions is presented in an interesting memoir by Hurwitz 'Über die Kettenbrüche deren Teilnenner arithmetische Reihen bilden' [28] (the contents of which is also reproduced in Perron [69], ch. IV). Hurwitz considers simple continued fractions of the form

$$\omega = [a_1, a_2, \ldots, a_1, \overline{\varphi_1(m), \varphi_2(m), \ldots, \varphi_k(m)}], \qquad (50)$$

where $\varphi_1(m), \ldots, \varphi_k(m)$ are integral polynomials in m (or, in particular, constant), and $\overline{\varphi_1(m), \varphi_2(m), \ldots, \varphi_k(m)}$ denotes the sequence of numbers

$$\varphi_1(1), \varphi_2(1), \ldots, \varphi_k(1), \quad \varphi_1(2), \ldots, \varphi_k(2), \quad \varphi_1(3), \ldots, \varphi_k(3), \ldots.$$

A periodic fraction is, clearly, a particular case of the fraction (50). For example, continued fractions for e and $\sqrt[s]{e}$ are of a form similar to (50)(e is the base of natural logarithms, s is an integer > 1):

$$e = [2, 1, 2, 1, 1, 4, 1, 1, 6, 1, \ldots],$$
$$\sqrt[s]{e} = [1, s-1, 1, 1, 3s-1, 1, 1, 5s-1, 1, 1, 7s-1, 1, \ldots].$$

Hurwitz shows that if an irrational number ω is decomposable into a continued fraction of the form (50), then $(a\omega+b)/(c\omega+d)$ where a, b, c, d are integers with determinant $ad-bc \neq 0$, may be expressed as a continued fraction of the same kind.

---

* Translator's note:

More precizely the idoneal numbers are the positive numbers Δ such that every genus of binary integral quadratic forms of discriminant Δ contains only one class. Chowla and Briggs (Canadian J. of Math. 1954, 463–470) shown that there are only finitely many of them but it has not been proved that there are no more than these listed.

3. POWER RESIDUES

§ 1. Gauss's first proof of the quadratic reciprocity law

The present chapter gives an exposition of elementary facts (i.e. facts which do not require the introduction of algebraic numbers) concerning the power residues to a prime modulus (§ 6, ch. I). First let us consider the simplest case – the quadratic residues, and study Gauss's first proof of the law of quadratic reciprocity. which presents a remarkable application of the principle of mathematical induction. (D. A. [20], art. 135–144, L. Dirichlet [14], § 48–51).

The outline of the proof is as follows: assuming the reciprocity law (theorem 7) to be proved for some pair of odd primes less than a given prime q, the theorem is then proved for q and any prime p which is less than q. Since for primes 3 and 5 the theorem is, true it follows that the theorem is, in general, true. We assume that the first auxilliary theorem to the reciprocity law is proven, i.e. $(-1/q) = (-1)^{\frac{1}{2}(q-1)}$ and that the same is true for the corresponding equalities for Jacobi symbols. Note that if theorem 7 is true for primes less than q, then a similar theorem is true for the Jacobi symbol (P/Q) $(Q/P) = (-1)^{\frac{1}{2}(P-1)\frac{1}{2}(Q-1)}$ if P, Q are odd relatively prime numbers (at least one of which is positive) and all their prime factors are less than q.

Thus, let theorem 7 be true for every pair of primes less than q; take any prime $p > 2$ and $< q$, and let us prove the equality (p/q) $(q/p) = (-1)^{\frac{1}{2}(p-1)\frac{1}{2}(q-1)}$. Leaving aside for the moment the case $q \equiv 1 \pmod 4$, $(p/q) = -1$, we assume in the remaining cases $r = p$ for $q \equiv \pm 1 \pmod 4$, $(p/q) = 1$ and $r = -p$ for $q \equiv 3 \pmod 4$, $(p/q) = -1$. Then $r = \pm p$ is a quadratic residue of q and the equality we are to prove is reduced to the following

$$\left(\frac{q}{r}\right) = (-1)^{\frac{1}{2}(q-1)\frac{1}{2}(r-1)}. \tag{1}$$

Since $(r/q) = 1$, there exists an *even* number $e > 0$ and $< q$, such that $e^2 - r = qf$, where f is an integer. The number f is: 1) odd, 2) positive (since for $f < 0$ we have $r > 0$, $r = p = e^2 + q$, $|f| > q$ which contradicts the hypothesis) 3) $f < q$ (since $qf \leqq e^2 + p < (q-1)^2 + (q-1) = q(q-1)$). If f is not divisible by p, then from equality $e^2 - r = qf$ (taking into account the fact that $f > 0$ and r are odd relatively prime numbers whose prime factors are all less than q), we obtain $(q/r) = (f/r) = (-1)^{\frac{1}{2}(f-1)\frac{1}{2}(r-1)}(r/f) = (-1)^{\frac{1}{2}(f-1)\frac{1}{2}(r-1)}$; but since e is odd, we have $-r \equiv qf$, $f \equiv -qr \pmod 4$ therefore $(q/r) = (-1)^{\frac{1}{2}(-qr-1)\frac{1}{2}(r-1)} = (-1)^{\frac{1}{2}(q-1)\cdot\frac{1}{2}(r-1)}$ i.e. equality (1) is proved for the present case. If $f \equiv 0 \pmod p$, then take $f = rf'$, $e = re'$ which gives $re' - 1 = qf'$, hence f' is not divisible by p. Numbers $-f'$ and r are odd, relatively prime, their absolute values are less than q, and they are of opposite sign (so that one of them is positive); Consequently, from $re'^2 - 1 = qf'$ we obtain $(q/r) = (-f'/r) = (-1)^{\frac{1}{2}(f'+1)\cdot\frac{1}{2}(r-1)}(r/f') = (-1)^{\frac{1}{2}(f'+1)\cdot\frac{1}{2}(r-1)}$. Further, since e' is even, we have $-1 \equiv qf'$, $f' \equiv -q \pmod 4$ and $(q/r) = (-1)^{\frac{1}{2}(q-1)\cdot\frac{1}{2}(r-1)}$. Therefore, formula (1) is proved for the cases considered.

Let us consider the case $q \equiv 1 \pmod 4$, $(p/q) = -1$ which was omitted before. In this case, to perform reasonings similar to the above we must show that there exists a prime p' less than q for which q is a quadratic non-residue. If $q \equiv 5 \pmod 8$ then $\frac{1}{2}(q+1)$ is a positive integer of the form $4n+3$, which is less than q, and has at least one prime factor of the same form $4n+3$. Since $q \equiv -1 \pmod{p'}$ and $p' \equiv -1 \pmod 4$ we have $(q/p') = -1$. If $q \equiv 1 \pmod 8$, then it is much more difficult to prove the existence of a prime p', and Gauss achieves it by means of the following brilliant deduction. Let $2m+1$ be a positive odd number, which is less than q and has the property that q is a quadratic residue of every odd prime less or equal to $2m+1$. Since $q \equiv 1 \pmod 8$, q is a quadratic residue of any power of 2 (§ 9, ch. I) and we may find an integer k, satisfying the congruence $q \equiv k^2 \pmod M$, where $M = 1, 2, 3, \ldots (2m+1)$. Since q is a prime and since $2m+1 < q$, we have $(k, M) = 1$. Further

$$k(q-1^2)(q-2^2)\ldots(q-m^2) \equiv k(k^2-1^2)(k^2-2^2)\ldots(k^2-m^2)$$
$$= (k-m)(k-m+1)\ldots(k-1)k(k+1)\ldots(k+m) \pmod M. \quad (2)$$

Since the product of $2m+1$ consecutive integers is divisible by a product of the same number of the first integers (§ 3 ch. I). The right

hand side of (2) is divisible by M. Taking into account the fact that $(k, M) = 1$, we can verify that the following number is an integer:

$$\frac{(q-1^2)(q-2^2)\dots(q-m^2)}{M} =$$

$$= \frac{1}{m+1}\cdot\frac{q-1^2}{(m+1)^2-1^2}\cdot\frac{q-2^2}{(m+1)^2-2^2}\cdots\frac{q-m^2}{(m+1)^2-m^2}. \qquad (3)$$

If we take $m = [\sqrt{q}]$, i.e. $m < \sqrt{q} < m+1$ (since $q \geqq 17$ we have $2\sqrt{q}+1 < q$), then the number (3) cannot be an integer, since it is the product of several positive proper fractions; with such choice of m our original supposition cannot take place, and we obtain the following theorem: *every prime q of the form $8n+1$ is a quadratic nonresidue for at least one odd prime not exceeding $2\sqrt{q}+1$.*

Returning to the last case in the proof of the law of reciprocity, i.e. $q \equiv 1 \pmod 4$, $(p/q) = -1$ $(2 < p < q$, p a prime) we find (by the lemma) a prime $p' < q$ for which $(p/q') = -1$. If $(p'/q) = 1$, then the pair of numbers p', q belongs to one of the cases of the reciprocity law given above, and we have $(q/p') = 1$, which contradicts the choice of p'. Consequently, $(p'/q) = -1$ and the law of reciprocity is established for the pair of numbers p', q. This enables us to assume the above prime p to be distinct from p'; moreover, equality $(q/p) = -1$ which we want to prove (and which expresses the reciprocity law for pair p, q) is equivalent to the following: $(q/pp') = +1$. Since pp' is a quadratic residue of q, we find an even number $e > 0$ and $< q$ for which $e^2 - pp' = qf$ (f is an odd integer, whose absolute value is less than q). If $(f, pp') = 1$), then since the reciprocity law is true for numbers pp', f we find

$$\left(\frac{q}{pp'}\right) = \left(\frac{f}{pp'}\right) = (-1)^{\frac{1}{2}(f-1)\cdot\frac{1}{2}(pp'-1)}, \quad \left(\frac{pp'}{f}\right) = (-1)^{\frac{1}{2}(f-1)\cdot\frac{1}{2}(pp'-1)}$$

and, since e is even, and $q \equiv 1 \pmod 4$, we have $f \equiv -pp' \pmod 4$ and $(q/pp') = (-1)^{\frac{1}{2}(-pp'-1)\frac{1}{2}(pp'-1)} = +1$ q.e.d. If f is divisible by one (and only one) of primes p, p' we can assume by symmetry that $f = pf'$, $e = pe'$, $pe'^2 - p' = qf'$, f' odd, $|f'| < q$, $(f', pp') = 1$, e' even. From $pe'^2 - p' = qf'$, since the reciprocity law holds for pairs $-p', p$ and pp', f' we find

$$\left(\frac{q}{pp'}\right) = \left(\frac{q}{p}\right)\left(\frac{q}{p'}\right) = \left(\frac{-p'f'}{p}\right)\left(\frac{pf'}{p'}\right) = \left(\frac{-p'}{p}\right)\left(\frac{p}{-p'}\right)\left(\frac{f}{pp'}\right)$$
$$= (-1)^{\frac{1}{2}(p-1)\cdot\frac{1}{2}(p'+1)+\frac{1}{2}(f'-1)\cdot\frac{1}{2}(pp'-1)}\left(\frac{pp'}{f}\right)$$
$$= (-1)^{\frac{1}{2}(p-1)\cdot\frac{1}{2}(p'+1)+\frac{1}{2}(f'-1)\cdot\frac{1}{2}(pp'-1)}.$$

But $f' \equiv -p' \pmod 4$, consequently,

$$\frac{f'-1}{2}\cdot\frac{pp'-1}{2} \equiv -\frac{p'+1}{2}\left(\frac{p-1}{2}+\frac{p'-1}{2}\right) \equiv \frac{p-1}{2}\cdot\frac{p'+1}{2} \pmod 2$$

and, again, we obtain $(q|pp') = 1$. Finally, when f is divisible by both p and p', we assume $f = pp'f'$, $e = pp'e'$, $pp'e'^2 - 1 = qf'$, f' – odd, $|f'| < q$, $(f, pp') = 1, e'$ – even. Applying the reciprocity law to numbers $-f'$ and pp' and noting that $-1 \equiv qf' \equiv f' \pmod 4$ we find from $pp'e'^2 - 1 = qf'$: $(q|pp') = (-f'|pp') = (-1)^{\frac{1}{2}(f'+1)\cdot\frac{1}{2}(pp'-1)}(pp'|f') = 1$. Thus, the law of reciprocity is completely proved.

§ 2. Distribution of power residues in a progression

In the present chapter we give an exposition on a memoir of academician I. M. Vinogradov 'Elementary proof of a general theorem of the analytical theory of numbers' [87]. Let p be an odd prime, and let $e > 1$ be a divisor of $p-1$. In § 6 of chapter 1 we have shown that the system of residues $1, 2, \ldots, p-1$ splits into e classes $A_0, A_1, \ldots, A_{e-1}$ with $(p-1)/e$ numbers in each class, where A_0 consists of all residues of degree e to *modulus* p, and non-residues of degree e are distributed among the classes $A_1, A_2, \ldots, A_{e-1}$. A class A_i may also be defined as a set of all numbers of a reduced system of residues, whose indices (to a fixed primitive root) are congruent to i *modulo* e. In the above-mentioned memoir, Vinogradov uses very ingenious and purely arithmetical reasonings to obtain an approximate formula for the number of elements of a class which are contained in the arithmetical progression $ax+b, x = 0, 1, 2, \ldots, h-1$ $(0 < h < p$, whose difference a is not divisible by p. First, we prove a few lemmas.

LEMMA I. *Let A, B be real numbers, let k be an integer, greater than zero, and let $A = t/q + \theta/qk$ (see theorem 8), where $0 < q \leqq k$, $(t, q) = 1$, and $|\theta| < 1$; if c and m are integers, and $0 < m \leqq k/q$, then*

$$\sum_{x=c}^{c+mq-1} \{Ax+B\} = \tfrac{1}{2}mq + \tfrac{1}{2}\rho(m+1), \qquad |\rho| \leqq 1, \tag{4}$$

As usual, the symbol $\{z\}$ denotes the fractional part of number z, and the sum on the left hand side is taken over all integers x within the given limits. Substituting instead of A its value we find $Ax+B = (tx+f(x))/q$, where $f(x) = Bq+\theta x/k$. Since $f(x)$ is a linear function of x, its values for $x = c,\ c+1, \ldots, c+mq-1$ are contained between the end values $f(c)$ and $f(c+mq-1)$; the difference between these numbers, i.e. $\theta(mq-1)/k$ is less in absolute value than 1. Consequently, the integers $[f(c)]$ and $[f(c+mq-1)]$ are either both equal, or their difference is equal to one. Let us split the sum S in the left hand side of (4) into m sums:

$$S = S_0+S_1+\ldots+S_{m-1}, \quad S_i = \sum_{c+iq}^{c+iq+q-1} \{Ax+B\},$$

and let us consider one of them, S_i say. If $[f(c+iq)] = [f(c+iq+q-1)] = n$ then, taking $f(x) = n+\lambda(x)\,[0 \leqq \lambda(x) < 1$ for $x = c+iq, c+iq+1, \ldots, c+iq+q-1]$, we have $S_i = \sum_{c+iq}^{c+iq+q-1}\{(tx+n+\lambda(x))/q\}$, expression $tx+n$ in this sum runs through a complete system of residues modulo q, therefore, denoting by r the least non-negative residue $tx+n$ modulo q, we have $S_i = \sum_{r=0}^{q-1}\{(r+\lambda(x))/q\} = \sum_{r=0}^{q-1}(r+\lambda(x))/q = \frac{1}{2}(q-1)+\theta = \frac{1}{2}q+\frac{1}{2}\rho_i$, $(0 \leqq \theta < 1, |\rho_i| \leqq 1)$. If, for the sum S_i, the difference between $[f(c+iq)]$ and $[f(c+iq+q-1)]$ is equal to one, then, denoting the least of these numbers by n and assuming again $f(x) = n+\lambda(x)$, we have $0 \leqq \lambda(x) < 2$ for $x = c+iq, \ldots, c+iq+q-1$ where the end values $\lambda(c+iq)$ and $\lambda(c+iq+q-1)$ satisfy the following inequalities: one of them is < 1 and the other $\geqq 1$ and < 2. Similarly to the above, we find

$$S_i = \sum_{c+iq}^{c+iq+q-1} \left\{\frac{tx+n+\lambda(x)}{q}\right\} = \sum_{r=0}^{q-1} \left\{\frac{r+\lambda(x)}{q}\right\}.$$

For $r = 0, 1, 2, \ldots, q-2$ we have, again $\{(r+\lambda(x))/q\} = (r+\lambda(x))/q$ and only for $r = q-1$, if the corresponding value of x satisfies inequality $1 \leqq \lambda(x) < 2$, we have $\{(r+\lambda(x))/q\} = (r+\lambda(x))/q-1$. Therefore, denoting a zero or a one by ε, we obtain

$$S_i = \sum_{r=0}^{q-1} \frac{r+\lambda(x)}{q} - \varepsilon = \frac{q-1}{2} - \varepsilon + \frac{1}{q} \sum_{c+iq}^{c+iq+q-1} \lambda(x)$$

$$= \frac{q}{2} - \tfrac{1}{2} - \varepsilon + \tfrac{1}{2}(\lambda(c+iq)+\lambda(c+iq+q-1)),$$

and, by the above inequalities for $\lambda(x)$, we have $S_i = \frac{1}{2}q+\rho_i$ where $|\rho_i| \leqq 1$. Noting that there is only one value of i for which $[f(c+iq)]$ and $[f(c+iq+q-1)]$ differ by one, and adding the expressions for $S_i (i = 0, 1, \ldots, m-1)$, we arrive at formula (4).

LEMMA II. *Let p be a prime, greater than 2; let α be one of numbers $1, 2, \ldots, p-1$, let β_α be an integer which may change as α varies, and let h be an integer > 0 and $< p$.*

Then, taking

$$S_\alpha = \sum_{x=0}^{h-1} \left\{\frac{\alpha x+\beta_\alpha}{p}\right\} \quad \text{and} \quad L_\alpha = S_\alpha - \tfrac{1}{2}h,$$

we have

$$\sum_{\alpha=1}^{p-1} |L_\alpha| < T \quad \text{where} \quad T = \sum_{x=1}^{h} \sum_{y} \left(\frac{p}{xy}+1\right), \tag{5}$$

and where in the sum T the summation for every x is performed over all y from the sequence $1, 2, \ldots, [p/x]$ which are relatively prime to x.

Considering one of the sums S_α, we find by theorem 8 an irreducible fraction t_0/x_0 satisfying the conditions $\alpha/p = t_0/x_0+\theta_0/x_0 h, 0 < x_0 \leqq h, |\theta_0| < 1$. Taking $m_0 = [h/x_0]$, $h_1 = h-m_0x_0$ $(m_0 > 0, 0 < h_1 < x_0)$ and splitting S_α into two parts $S_\alpha = \sum_{x=0}^{m_0x_0-1}\{(\alpha x+\beta_\alpha)/p\} + \sum_{m_0x_0}^{h-1}\{(\alpha x+\beta_\alpha)/p\}$ we note that lemma I may be applied to the first part of the sum S_α (taking $q = x_0$). Using formula (4), and taking into consideration the fact that $m_0x_0 = h-h_1$, $m_0 \leqq h/x_0$, we find the following expression for the sum S_α:

$$S_\alpha = \tfrac{1}{2}(h-h_1)+\tfrac{1}{2}\rho_0\left(\frac{h}{x_0}+1\right)+S'_\alpha, \qquad |\rho_0| \leqq 1,$$

$$S'_\alpha = \sum_{x=c_0}^{c_0+h_1-1} \left\{\frac{\alpha x+\beta_\alpha}{p}\right\}, \qquad c_0 = m_0x_0.$$

The sum S'_α is then treated similarly. Assume by theorem 8

$$\frac{\alpha}{p} = \frac{t_1}{x_1} + \frac{\theta_1}{x_1h_1}, \qquad 0 < x_1 \leqq h_1, \quad (t_1, x_1) = 1, \quad |\theta_1| < 1,$$

$$m_1 = \left[\frac{h_1}{x_1}\right], \quad h_2 = h_1-m_1x_1, \qquad 0 < h_2 < x_1,$$

and repeating the process for S'_α we obtain the expression:

$$S'_\alpha = \tfrac{1}{2}(h_1 - h_2) + \tfrac{1}{2}\rho_1 \left(\frac{h_1}{x_1} + 1\right) + S''_\alpha, \qquad |\rho_1| \leqq 1,$$

$$S''_\alpha = \sum_{x=c_1}^{c_1+h_2-1} \left\{\frac{\alpha x + \beta_\alpha}{p}\right\}, \qquad c_1 = m_0 x_0 + m_1 x_1 .$$

Continue the algorithm further; inequalities $0 < h_1 < x_0 \leqq h$, $0 < h_2 < x_1 \leqq h_1$ show that the sequence $h, h_1, h_2, \ldots$ is strictly decreasing and therefore, at some step, we shall have $h_{n+1} = 0$ and this is where the algorithm ends. The last equality is of the form

$$S^{(n)}_\alpha = \tfrac{1}{2}h_n + \tfrac{1}{2}\rho_n \left(\frac{h_n}{x_n} + 1\right), \qquad |\rho_n| \leqq 1,$$

where, as before $\alpha/p = t_n/x_n + \theta_n/x_n h_n$, $0 < x_n \leqq h_n$, $(t_n, x_n) = 1$, $|\theta_n| < 1$, $m_n = [h_n/x_n] = h_n/x_n$, $h_{n+1} = h_n - m_n x_n = 0$. Adding the expressions for S_α, $S'_\alpha, \ldots, S^{(n)}_\alpha$ we obtain

$$S_\alpha = \tfrac{1}{2}h + \tfrac{1}{2}\rho_0 \left(\frac{h}{x_0} + 1\right) + \tfrac{1}{2}\rho_1 \left(\frac{h_1}{x_1} + 1\right) + \ldots + \tfrac{1}{2}\rho_n \left(\frac{h_n}{x_n} + 1\right),$$

from which

$$L_\alpha = S_\alpha - \tfrac{1}{2}h = \tfrac{1}{2}\rho \left(\left(\frac{h}{x_0} + 1\right) + \left(\frac{h_1}{x_1} + 1\right) + \ldots + \left(\frac{h_n}{x_n} + 1\right)\right), \qquad |\rho| \leqq 1,$$

and

$$\sum_{\alpha=1}^{p-1} |L_\alpha| \leqq \tfrac{1}{2} \sum_{\alpha=1}^{p-1} \left(\left(\frac{h}{x_0} + 1\right) + \left(\frac{h_1}{x_1} + 1\right) + \ldots + \left(\frac{h_n}{x_n} + 1\right)\right). \quad (6)$$

In the latter sum it is assumed that the numbers $x_0, h_1, x_1, h_2, \ldots$ and n are defined for every α, and then the summation is performed over all α. To estimate the value of this sum, we collect together all its terms of the form $h_i/x_i + 1$ with the same x_i. Rewriting the equality $\alpha/p = t_i/x_i + \theta_i/x_i h_i$ in the form $\alpha x_i = pt_i + y_i$ $(y_i = p\theta_i/h_i)$, we see that y_i is an integer, relatively prime to x_i, satisfying the conditions $\alpha x_i \equiv y_i \pmod p$, $0 < |y_i| < p/h_i$. Conversely, if the given numbers x_i, y_i (for fixed α and h_i), satisfy the above conditions, then they define number t_i. To find the upper bound of the sum of all those terms

h_i/x_i+1 in which x_i is a given number x $(0 < x \leqq h)$, we consider the values α and y_i corresponding to them. It follows from $0 < |y_i| < p/h_i \leqq p/x_i$ that y_i may take only those values $\pm 1, \pm 2, \ldots, \pm[p/x]$ which are relatively prime to x. For a fixed y_i the corresponding value of α is defined from the congruence $\alpha x_i \equiv y_i \pmod p$. Further, $h_i/x_i < p/x|y_i|$ and thus the sum of the terms h_i/x_i+1 is not greater than $2\sum(p/xy+1)$, where the summation is performed over all y from the sequence $1, 2, \ldots, [p/x]$ which are relatively prime to x. Therefore, the right hand side of (6) does not exceed the sum T, which proves lemma II.

LEMMA III. *Let the numbers p, α, β_α be the same as in the previous lemma; moreover, let h and γ be integers, greater than zero and less than p. Denote by R_α the number of integers $\alpha x+\beta_\alpha$ $(x = 0, 1, 2, \ldots, h-1)$ whose least residues modulo p are greater or equal to zero and less than γ, and assume $H(\alpha, \beta_\alpha, h, \gamma) = R_\alpha - h\gamma/p$. Then*

$$\sum_{\alpha=1}^{p-1} |H(\alpha, \beta_\alpha, h, \gamma)| < 2T,$$

where T has the same meaning as in the previous lemma. (See (5)).

This lemma follows directly from the previous one. Noting that $\{(\alpha x+\beta_\alpha-\gamma)/p\} - \{(\alpha x+\beta_\alpha)/p\} = 1-\gamma/p$ when the least residue of $\alpha x+\beta_\alpha$ modulo p is $\geqq 0$ and $< \gamma$, and $= -\gamma/p$ when the least residue is $\geqq \gamma$ and $< p$, we obtain

$$S'_\alpha - S_\alpha = \sum_{x=0}^{h-1} \left\{\frac{\alpha x+\beta_\alpha-\gamma}{p}\right\} - \sum_{x=0}^{h-1} \left\{\frac{\alpha x+\beta_\alpha}{p}\right\} = R_\alpha - \frac{h\gamma}{p} = H(\alpha, \beta_\alpha, h, \gamma).$$

But, from the previous lemma

$$\sum_{\alpha=1}^{p-1} \left| S'_\alpha - \frac{h}{2} \right| < T, \quad \sum_{\alpha=1}^{p-1} \left| S_\alpha - \frac{h}{2} \right| < T,$$

from which

$$\sum_{\alpha=1}^{p-1} |S'_\alpha - S_\alpha| = \sum_{\alpha=1}^{p-1} |H(\alpha, \beta_\alpha, h, \gamma)| < 2T,$$

q.e.d.

Now we can formulate the above mentioned theorem of Vinogradov as follows

Let p be an odd prime, let $e > 1$ be a divisor of $p-1$, and let numbers $1, 2, \ldots, p-1$ be split into classes $A_0, A_1, \ldots, A_{e-1}$ of residues and non-residues of degree e modulo p (see above). If a is a number, not divisible by p, b is an arbitrary integer, and $0 < h < p$, then the number c_i of the elements of the i-th class A_i (for an arbitrary i), contained in progression $ax+b$ ($x = 0, 1, 2, \ldots, h-1$), is representable in the form $c_i = h/e + \Delta_i$, where $\Delta_i^2 < 2T$ and T (the same as in lemmas II and III) *is defined by formula* (5).

Let i be one of the numbers $0, 1, 2, \ldots, e-1$; let us construct $((p-1)/e)h$ products

$$\alpha(ax+b) \qquad (7)$$

where α runs through all the numbers of class A_i and, independently of α, $x = 0, 1, 2, \ldots, h-1$. For every such product, we define a number u by means of a congruence $au+b \equiv \alpha(ax+b) \pmod p$ where $0 \leqq u < p$, and denote by D the number of products (7) for which the corresponding values of u are less than h. The proof of the theorem is based on the evaluation of D by two different methods. First, consider the products (7) which correspond to the same value of α. Assuming $aa' \equiv 1 \pmod p$, we may replace the congruence for u by the following $u \equiv \alpha x + \beta_\alpha \pmod p$ where $\beta_\alpha = \alpha ba' - ba'$ is independent of x. Thus, by the notations of lemma III, the part of D corresponding to the constant α may be represented in the form $h^2/p + H(\alpha, \beta_\alpha, h, h)$; summing these values over all α, we find

$$D = \frac{p-1}{e}\,\frac{h^2}{p} + \sum_\alpha H(\alpha, \beta_\alpha, h, h).$$

Let us now evaluate D by another method, assuming x to be constant in the products (7). If, for a given x we have $ax+b \equiv 0 \pmod p$, then all $(p-1)/e$ of the corresponding products (7) must be counted as belonging to D. However, if for a given x the number $ax+b$ is one of the c_j numbers of class A_j, contained in the given progression $ay+b$ ($y = 0, 1, \ldots, h-1$) then the number $au+b$ in the congruence $au+b \equiv \alpha(ax+b) \pmod p$ belongs to class A_{i+j}, and it is easy to see that among all numbers α there exist c_{i+j} numbers for which $0 \leqq u < h$ (we count $c_k = c_n$ for $k \equiv n \pmod e$). Hence

$$D = c_0 c_i + c_1 c_{i+1} + \ldots + c_{e-1} c_{i+e-1} + \eta,$$

where $\eta = (p-1)/e$ if the progression $ay+b$ ($y = 0, 1, \ldots, h-1$)

contains 0, and $\eta = 0$ otherwise. Comparing expressions for D we obtain for every i

$$c_0 c_i + c_1 c_{i+1} + \ldots + c_{e-1} c_{i+e-1} + \eta = \\ = \frac{p-1}{e} \frac{h^2}{p} + \sum_{\alpha} H(\alpha, \beta_\alpha, h, h), \qquad (8)$$

where on the right hand side the summation is performed over all numbers α of class A_i. Take in (8) $i = 0$ and subtract formula (8) term by term from the obtained formula. Taking into account the fact that the numbers $c_i, c_{i+1}, \ldots, c_{i+e-1}$ are numbers $c_0, c_1, \ldots, c_{e-1}$ written in different order, we obtain

$$(c_0 - c_i)^2 + (c_1 - c_{i+1})^2 + \ldots + (c_{e-1} - c_{i+e-1})^2 = \\ = 2 \sum_{\alpha'} H(\alpha', \beta_{\alpha'}, h, h) - 2 \sum_{\alpha} H(\alpha, \beta_\alpha, h, h),$$

where in the right hand side α and α' run through all the elements of classes A_i and A_0 respectively. It follows from lemma III, that the right hand side of the latter equality does not exceed $4T$, and therefore for every r, we have $(c_r - c_{r+i})^2 + (c_r - c_{r-i})^2 < 4T$ adding these inequalities for all $i = 1, 2, \ldots, e-1$ with an obvious equality $(c_r - c_r)^2 + (c_r - c_r)^2 = 0$ we find $2 \sum_{i=0}^{e-1} (c_r - c_i)^2 < 4T(e-1)$. Take $(c_0 + c_1 + \ldots + c_{e-1})/e \leqq g$, $c_i = g + \delta_i$ $(i = 0, 1, \ldots, e-1)$; then $\sum_{i=0}^{e-1} (\delta_r - \delta_i)^2 < 2T(e-1)$ and since $\delta_0 + \delta_1 + \ldots + \delta_{e-1} = 0$ we have $e\delta_r^2 + \sum_{i=0}^{e-1} \delta_i^2 < 2T(e-1)$ from which $\delta_r^2 < 2T(e-1)/(e+1)$. If the given progression $ax + b$ $(x = 0, 1, \ldots, n-1)$ does not contain zero, clearly $g = h/e$, $\delta_r = \Delta_r$ and $\Delta_r^2 < 2T(e-1)/(e+1) < 2T$. If the progression contains zero to modulus p, then $g = (h-1)/e$, $\Delta_r = \delta_r - 1/e$, $\Delta_r^2 < 2T(e-1)/(e+1) + (2|\delta_r|)/e$. But we see from $\delta_i = c_i - g$, that $|\delta_i| < \frac{1}{2}p < \frac{1}{2}T$ from which $\Delta_r^2 < 2T((e-1)/(e+1) + 1/2e) < 2T$, Thus, the theorem is proved.

From this theorem we may easily deduce another theorem of I. M. Vinogradov on the distribution of primitive roots in a progression. The proof of this theorem is based on the following simple statement: let M be any collection of integers (a finite number); denote by N_e the number of those integers of M which are divisible by e. Then for any integer $n > 0$, the sum $\sum \mu(e) N_e$ taken over all the divisors e of n represents the number of integers of M which are relative prime to n. This statement can be easily proved by using the Möbius function

$\mu(e)$ (§ 2, ch. 1). Consider a progression $ax+b$ ($x = 0, 1, \ldots, h-1$, $0 < h < p$) and, omitting the number $\equiv 0 \pmod p$ if it is contained in this progression, take the indices of all the remaining numbers to some primitive root. Assume the totality of these indices to be M of the previous statement, and take $n = p-1$. Since every number whose index is relatively prime to $p-1$, is a primitive root of p, it follows that the number G of primitive roots in a given progression may be expressed as follows: $G = \sum \mu(e) N_e$, where the summation is performed over all the divisors e of $p-1$, and N_e denotes the number of elements of the given progression whose indices are divisible by e, i.e. the number of residues of degree e modulo p. For $e > 1$, it follows from the above theorem that $N_e = h/e + \rho_e \sqrt{2T}$, $|\rho_e| < 1$; for $e = 1$, N_1 is equal either to h or to $h-1$, and it may also be assumed that $N = h + \rho_1 \sqrt{2T}$, $|\rho_1| < 1$. Consequently, $G = h \sum \mu(e)/e + \sqrt{2T} \sum \mu(e) \rho_e = h(\varphi(p-1))/(p-1) + \sqrt{2T} \sum \mu(e) \rho_e$ where $\varphi(n)$ is the Euler function (§ 2, ch. 1). Noting that $\mu(e) = 0$ for e which is divisible by a square, and $\mu(e) = \pm 1$ otherwise, we obtain the required theorem: *The number of primitive roots in a given arithmetical progression* $ax+b$ ($x = 0, 1, \ldots, h-1$, $0 < h < p$) *may be represented in the form* $h(\varphi(p-1))/(p-1) + \rho \cdot 2^{\nu} \sqrt{2T}$ *where* $|\rho| < 1$ *and* ν *denotes the number of distinct prime divisors of* $p-1$. A similar theorem may be deduced for numbers belonging to a given exponent modulo p (see note to § 6, ch. 1). Concerning the quantity T, a rough estimation shows that it is of order $p(\log p)^2$ so that the orders of supplementary terms in the above formulas for the number of power residues and that of primitive roots in a progression are, respectively, $\sqrt{p} \log p$, and $2^{\nu} \sqrt{p} \log p$. *

§ 3. Biquadratic residues; criteria for a number to belong to a biquadratic distribution class

After quadratic residues, the simplest power residues are biquadratic and cubic residues. Gauss, who began the study of these residues in 1805, soon noticed their characteristic property: the proof and the expression of their main property – the reciprocity law cannot be performed by means of ordinary arithmetic. Only on expanding the domain of rational numbers (by adjoining to it the fourth root

* The work of L. A. Burgess improves these bounds to $0(p^{\frac{1}{2}}(\log p)^{\frac{1}{2}})$. See L. A. Burgess Proc. Lond. Math. Soc. 1962. 172–179.

$i = \sqrt{-1}$ of unity for biquadratic, and cubic roots of unity $\rho = \frac{1}{2}(-1+\sqrt{3})$ for cubic residues), we succeed in obtaining a finite expression for the biquadratic and cubic reciprocity law. The results obtained by means of ordinary arithmetic in the theory of biquadratic residues are described by Gauss in his memoir 'Theoria residuorum biquadraticorum', Comm. I, (see [20], p. 511). Some additions were later made by Dirichlet (see [13], vol. I, p. 63). This, and the subsequent sections give a brief survey of the results of Gauss and Dirichlet.

Let p be an odd prime. Clearly, for $p \equiv 3 \pmod 4$ every quadratic residue is at the same time a biquadratic residue; therefore we can speak of an independent theory of biquadratic residues (if we remain in the domain of ordinary integers) only for prime moduli of the form $4n+1$ and this assumption will be presumed for p throughout the present section. Taking a root f of congruence $x^4 \equiv 1 \pmod p$ distinct from ± 1 (for which, consequently, $f^2+1 \equiv 0$), we may divide all the numbers $1, 2, \ldots, p-1$ equally into four classes A, B, C, D (§ 6, ch. 1). By the reasoning of § 6, ch. 1, number a belongs to a class A, B, C, or D if in the congruence $a^{\frac{1}{4}(p-1)} \equiv f^{\alpha} \pmod p$ the exponent α is equal to $0, 1, 2, 3$ respectively. All biquadratic residues modulo p are contained in class A; further, it is clear, that classes A and C contain all quadratic residues, and classes B and D – all quadratic nonresidues modulo p. On passing from f to another root $-f$ of congruence $f^2+1 \equiv 0 \pmod p$, the classes A and C remain unchanged, but classes B and D interchange places. Concerning the biquadratic residues, similarly to the quadratic residues there are two main problems: 1) to which class does a given number q belong to a given modulus p? This question is solved by means of the Euler congruence indicated above. The other, more difficult question is as follows: 2) for which prime moduli of the form $p = 4n+1$ does a given number q belong to a given class A, B, C, or D. The complete solution of this problem is achieved by means of the biquadratic law of reciprocity.

Since the class A, B, C, or D of a product is determined by those of its factors, it suffices to solve the second problem for $q = -1$, $q = 2$, and for the case when q is an odd prime. Concerning -1, it follows immediately from Euler's criterion that this number belongs to class A for $p \equiv 1 \pmod 8$ and to class C if $p \equiv 5 \pmod 8$. For the remaining values of q, finding in particular examples that a number $q = 2, 3, 5, \ldots$ belongs to classes A, B, C or D to moduli $p = 5, 13,$

17, 29, . . ., we find no direct connection between belonging to the class and the modulus p. This connection can only be noticed if, using Fermat theorem (§ 8, ch. 2), we represent p as a sum of two squares. Thus, let $p = a^2+4b^2$ where a and b are integers, defined uniquely for a given p (disregarding the sign).

In order to find a connection between number 2 belonging to classes A, B, C, D to modulus p and the numbers a, b, the root f of the congruence $f^2+1 \equiv 0 \pmod p$ has to be normalised in a special way, where f determines the decomposition into classes A, B, C, D. Taking into account the fact, that $(a/2b)^2+1 \equiv 0 \pmod p$ and, consequently that $a \equiv \pm 2bf$, choose root f by the condition $a+2bf \equiv 0 \pmod p$. From $(a+2b)^2 = a^2+4ab+b^2 = p+4ab$ we obtain

$$(a+2b)^{\frac{1}{4}(p-1)} \equiv 2^{\frac{1}{4}(p-1)}(2ab)^{\frac{1}{4}(p-1)}$$

and

$$2^{\frac{1}{4}(p-1)}(2ab)^{\frac{1}{4}(p-1)} \equiv \left(\frac{a+2b}{p}\right) \pmod p.$$

Further, from $a+2bf \equiv 0$ follows $2b \equiv af$, $(2ab)^{\frac{1}{4}(p-1)} \equiv a^{\frac{1}{4}(p-1)}f^{\frac{1}{4}(p-1)} \equiv (a/p)f^{\frac{1}{4}(p-1)}$, and, consequently, $2^{\frac{1}{4}(p-1)} \equiv f^{\frac{3}{4}(p-1)}(a/p)((a+2b)/p) \pmod p$. It is clear from $p = a^2+4b^2$ that p is a quadratic residue of an odd number a; consequently $(p/a) = 1$, and by the reciprocity law $(a/p) = 1$. Similarly, from $2p = (a+2b)^2+(a-2b)^2$ we obtain $(2/(a+2b)) = (p/(a+2b)) = ((a+2b)/p)$. Thus,

$$2^{\frac{1}{4}(p-1)} \equiv f^{\frac{3}{4}(p-1)}\left(\frac{2}{a+2b}\right)$$
$$= (-1)^{\frac{1}{8}((a+2b)^2-1)}f^{\frac{3}{4}(p-1)} \equiv f^{\frac{1}{4}(p-1+4ab)+\frac{1}{4}(p-1)} \equiv f^{ab} \pmod p,$$

and we obtain the following theorem: *let a, b be integers from equation $p = a^2+4b^2$ taken with arbitrary signs, and let f be the root of the congruence $f^2+1 \equiv 0 \pmod p$ chosen depending on a, b by the condition $a+2bf \equiv 0 \pmod p$. Then the number 2 belongs to class A, B, C or D (defined depending on root f) to modulus p, if $ab \equiv 0, 1, 2$ or $3 \pmod 4$.* Using representations of p by other quadratic forms, we may obtain similar criteria for 2. Let p be of the form $8n+1$. In § 8, ch. 2 we have seen that p is representable by either of the forms x^2+8y^2 and x^2-8y^2. Let $p = \alpha^2+8\beta^2$, $(\alpha > 0, \beta > 0)$; this representation is possible in one way only. We do not select the root f of the congruence $f^2+1 \equiv 0 \pmod p$ in this case, since for $p \equiv 1$

(mod 8) we have $(2/p) = 1$, and therefore 2 belongs to one of the classes A or C independent of the choice of f. From equation $p = \alpha^2 + 8\beta^2$ we find $2^{\frac{1}{2}(p-1)}\beta^{\frac{1}{2}(p-1)} \equiv \alpha^{\frac{1}{2}(p-1)}$ or $2^{\frac{1}{2}(p-1)} \equiv (\alpha/p)(\beta/p)$ (mod p); taking $\beta = 2^\nu\gamma$, $\nu \geqq 0$, γ – odd, we have $(p/\gamma) = 1$ from which $(\beta/p) = (2^\nu/p)(\gamma/p) = 1$. Further, from the equation $p = \alpha^2 - 8\beta^2$ we have $(p/\alpha) = (2/\alpha)$, $(\alpha/p) = (2/\alpha)$ so that $2^{\frac{1}{2}(p-1)} \equiv (2/\alpha)$ (mod p). We obtain the following theorem: *for a prime* $p = \alpha^2 + 8\beta^2$ *the number* 2 *belongs to class A if* $\alpha \equiv \pm 1$ *and to class C if* $\alpha \equiv \pm 3$ (mod 8).

Considering equation $p = \alpha^2 - 8\beta^2$, we obtain a similar result: *let* $\alpha > 0$ *and let* β *be any solution of equation* $p = \alpha^2 - 8\beta^2$ (*there is an infinity of such solutions, one of them satisfies* $\alpha > 4\beta > 0$, *see* § 8, *ch.* 2); 2 *belongs to class A modulo p if* $\alpha \equiv 1, 3$ *and to class C modulo p if* $\alpha \equiv 5,7$ (*mod* 8). Comparing these criteria with the above result leads to the following two theorems:

1) *For a prime p of the form* $8n+1$, *the numbers b and* α *in equations* $p = a^2 + 16b^2$, $p = \alpha^2 - 8\beta^2 (\alpha > 0)$, *are related as follows: if b is even, then* $\alpha \equiv \pm 1$ (*mod* 8), *if b is odd, then* $\alpha \equiv \pm 3$ (mod 8).

2) *For the same prime p in equations* $p = a^2 + 16b^2, p = \alpha^2 - 8\beta^2$ $(\alpha > 0)$, *the numbers b and* α *are related in such a way that if b is even, then* $\alpha \equiv 1$ *or* 3 (*mod* 8), *and if b is odd, then* $\alpha \equiv 5$ *or* 7 (mod 8). These theorems are interesting because they establish dependence between the representations of the same numbers by means of forms x^2+y^2, x^2+2y^2, x^2-2y^2 whose discriminants do not differ by a square, so that they may not be transformed into one another by means of a substitution with rational coefficients (§ 3, ch. 2). In chapter 5 we arrive at these theorems again by completely different reasonings, and prove them for any composite number of the form $8n+1$.

Consider the problem of finding to which class A, B, C or D does an odd prime $q \neq p$ belong modulo p. Again, assume $p = a^2 + b^2$ (a – odd) and choose a root f of congruence $f^2 + 1 \equiv 0$ (mod p) which provides the distribution into classes A, B, C, D under the condition $a + bf \equiv 0$ (mod p). Since the class to which -1 belongs is known, we may take $\pm q$ instead of q, choosing the sign by the condition $\pm q \equiv 1$ (mod 4). Working out for particular examples to which classes A, B, C, D the numbers -3, $+5$, -7, $-11, \ldots$ belong, we find that the criteria of belonging are always expressed by congruences of the form $a \equiv 0$ or $b \equiv ax$ (mod q) (from now on these congruences will be called the *conditional* congruences). For example, -3 belongs

to class A for such prime $p = a^2+b^2$ for which $b \equiv 0 \pmod 3$, to class B for such p for which $b \equiv -a \pmod 3$, to class C for $a \equiv 0 \pmod 3$ and to class D for $b \equiv a \pmod 3$. Here are some similar tables of criteria:

$+5$

A	$b \equiv 0$
B	$b \equiv a$
C	$a \equiv 0$
D	$b \equiv -a$

$(\mathrm{mod}\ 5)$

-1

A	$a \equiv 0,\ b \equiv 0$
B	$b \equiv -3a, -2a$
C	$b \equiv a, -a$
D	$b \equiv 3a, 2a$

$(\mathrm{mod}\ 7)$

-11

A	$b \equiv 0, \pm 5a$
B	$b \equiv a, 3a, 4a$
C	$a \equiv 0,\ b \equiv \pm 2a$
D	$b \equiv -a, -3a, -4a$

$(\mathrm{mod}\ 11)$

$+13$

A	$b \equiv 0, \pm 4a$
B	$b \equiv -a, -2a, 6a$
C	$a \equiv 0,\ b \equiv \pm 3a$
D	$b \equiv a, 2a, -6a$

$(\mathrm{mod}\ 13)$

Considering these tables we come to the following deductions: 1) *The fact that* $\pm q \equiv 1$ (*mod* 4) *belongs to a class A, B, C or D modulo p is established by means of conditional congruences of the form* $a \equiv 0$ *or* $b \equiv ax$ (*mod q*). 2) *Congruence* $b \equiv 0$ (*mod q*) *always enters in one of criteria for class A.* 3) *Congruence* $a \equiv 0$ (*mod q*) *is always one of the congruences of the criteria for class A when* $(2/q) = +1$, *and of those for class C when* $(2/q) = -1$. 4) *In the conditional congruences* $b \equiv ax$ (*mod q*), *the number x takes all the values* 0, 1, 2, . . ., $q-1$ *apart from two numbers which satisfy the congruence* $x^2+1 \equiv 0$ (*mod q*) *when it is solvable* (*i.e. when* $q \equiv 1$ (*mod* 4)). 5) *The number of conditional congruences for every class A, B, C, D is the same, namely it is* $\frac{1}{4}(q+(-1)^{\frac{1}{2}(q+1)})$. These theorems express nothing else but the part of the biquadratic reciprocity law which concerns rational integers.

In the above mentioned memoir of Dirichlet (see [13], vol. I. p. 63) it has been shown that theorems 1–5, *as far as they are concerned with classes A and C* may be proved by means of ordinary arithmetic. Dirichlet uses the following statement from the theory of quadratic forms: *if a prime* $\pm q \equiv 1 \pmod 4$ *is a quadratic residue of* $m > 0$, *relatively prime to* $2q$ *then there exists an even power* m^h *of this number, representable by the form* $x^2 \mp qy^2$ *with relatively prime x, y.* This statement is a direct consequence of the composition of quadratic forms,

which will be shown in chapter 4 (though it may be deduced elementarily by means of formulae (32) §8, ch. 2). Thus, restricting ourselves to classes A and C in theorems 1–5 let us assume that $(\pm q/p) = 1$; then, by the above statement, we have $p^h = t^2 \mp qu^2$, h – odd, $(t, u) = 1$, $t > 0$, $u > 0$. From which

$$(\pm q)^{\frac{1}{2}(p-1)} \equiv \left(\frac{t}{p}\right)\left(\frac{u}{p}\right) \pmod{p}.$$

Let us note that t is odd, and u is even; moreover, for $p \equiv 5 \pmod 8$, u is not divisible by 4. Taking $u = 2^\gamma v$, $\gamma > 0$ v – odd, greater than zero, we find from $p^h = t^2 \mp qu^2$ that $(\mp qp/t) = 1$, $(t/pq) = (-1)^{\frac{1}{2}(t-1)}$, $(t/p) = (-1)^{\frac{1}{2}(t-1)}(t/q)$, $(p/v) = 1$, $(u/p) = (2^\gamma/p)(v/p) = (2/p)$. Thus,

$$(\pm q)^{\frac{1}{2}(p-1)} \equiv (-1)^{\frac{1}{2}(t-1)}\left(\frac{2}{p}\right)\left(\frac{t}{q}\right) \pmod{p}. \tag{9}$$

Using the representation $p = a^2 + b^2$, it is easy to transform the equality $p^h = t^2 \mp qu^2$ into the following

$$(t + p^{\frac{1}{2}(h-1)}b)(t - p^{\frac{1}{2}(h-1)}b) = (p^{\frac{1}{2}(h-1)}a)^2 + qu^2. \tag{10}$$

Take $(a, u) = l$, $p^{\frac{1}{2}(h-1)}a = l\xi$, $u = l\eta$; then $(\xi, \eta) = 1$ and, since a is odd, l must be odd. By (10), since $t + p^{\frac{1}{2}(h-1)}b$, $t - b^{\frac{1}{2}(h-1)}b$ and l have no common divisor, we obtain

$$t + p^{\frac{1}{2}(h-1)}b = v^2 g, \quad (t - p^{\frac{1}{2}(h-1)}b = v'^2 g'),$$
$$(vv' = l), \quad gg' = \xi^2 \pm q\eta^2. \tag{11}$$

First, consider the case when $a \equiv 0 \pmod q$. In this case it is evident from (10) that one of the numbers $t + p^{\frac{1}{2}(h-1)}b$, $t - p^{\frac{1}{2}(h-1)}b$ is divisible by q, and another is not divisible by q. If, for example, $t + p^{\frac{1}{2}(h-1)}b \not\equiv 0 \pmod q$ then from (11) we have $(\mp q/g) = 1 = (\mp q/(t + p^{\frac{1}{2}(h-1)}b))$ and since for $\mp q < 0$, we have $t + p^{\frac{1}{2}(h-1)}b > 0$, the reciprocity law gives $((t + p^{\frac{1}{2}(h-1)})b)/q) = (-1)^{\frac{1}{2}(t-1)+\frac{1}{2}b} = (-1)^{\frac{1}{2}(t-1)}(2/p)$. Since $p^{\frac{1}{2}(h-1)}b \equiv t \pmod q$, it follows that $(2t/q) = (-1)^{\frac{1}{2}(t-1)}(2/p)$, so that the congruence (9) is of the form $(\pm q)^{\frac{1}{2}(p-1)} \equiv (2/q) \pmod p$. Thus, for $(\pm q/p) = 1$, and a divisible by q, the number $\pm q$ belongs to class A modulo p for $(2/q) = 1$, and to class C $(2/q) = -1$. But, since equality $(\pm q/p) = 1$ is a corollary of the supposition $a \equiv 0 \pmod q$, we obtain the proof of theorem 3 from the above theorems 1–5.

Now we may assume in (11) that a is not divisible by q. Then $t+p^{\frac{1}{2}(h-1)}b$ and $t-p^{\frac{1}{2}(h-1)}b$ are not divisible by q and form (11), similarly to the above, we obtain (for both signs) $((t\pm p^{\frac{1}{2}(h-1)}b)/q) = (-1)^{\frac{1}{2}(t-1)}(2/p)$. Since $(p/q) = 1$ we take any root σ of the congruence $x^2 \equiv p \pmod q$. From $p^h = t^2 \mp qu^2$ we find $t \equiv \varepsilon p^{\frac{1}{2}(h-1)}\sigma \pmod q$ and further, $(t/q) = (\varepsilon\sigma/q)$, $((t+\varepsilon p^{\frac{1}{2}(h-1)}b)/q) = (\varepsilon(\sigma+b)/q) = (t\sigma(\sigma+b)/q) = (-1)^{\frac{1}{2}(t-1)}(2/p)$, $(-1)^{\frac{1}{2}(t-1)}(2/p)(t/q) = (\sigma(\sigma+b)/q)$. Substituting this into congruence (9), we obtain the following result: if $(\pm q/p) = 1$, $a \not\equiv 0 \pmod q$ and if σ is a root of the congruence $p \equiv \sigma^2 \pmod q$ then

$$(\pm q)^{\frac{1}{2}(p-1)} \equiv \left(\frac{\sigma(\sigma+b)}{q}\right) \pmod p. \tag{12}$$

For $b = 0 \pmod q$ it follows directly from the above congruence that $\pm q$ belongs to class A modulo p, i.e. we obtain the proof of theorem 2. Define numbers x and τ from congruences $b \equiv ax$, $\sigma \equiv a\tau \pmod q$; then the congruence $p \equiv \sigma^2 \pmod q$ may be replaced by the following: $\tau^2 - x^2 \equiv 1 \pmod q$. Taking $\tau + x \equiv k \not\equiv 0 \pmod q$, we obtain $2x \equiv k - 1/k$, $2\tau \equiv k + 1/k \pmod q$ from which $(\sigma(\sigma+b)/q) = (\tau(\tau+x)/q) = (2/q)((k^2+1)/q)$. Substituting this into (12) we obtain the following rule for determining to which class modulo p number $\pm q$ belongs (in the case $(\pm q/p) = 1$ and $a \not\equiv 0 \pmod q$). Defining x by the condition $b \equiv ax \pmod q$ we see that $x^2 + 1 \equiv p/a^2 \pmod q$ is a quadratic residue modulo q, not divisible by q. Under this condition the congruence $2x \equiv k - 1/k \pmod q$ has, clearly, two solutions with respect to k; since these solutions are connected by a relation $kk' \equiv -1 \pmod q$ we find that k^2+1 and k'^2+1 (both $\not\equiv 0 \pmod q$) have the same quadratic character modulo q. Moreover, $\pm q$ belongs to class A modulo p if $((k^2+1)/q) = (2/q)$ and to class C if $((k^2+1)/q) = -(2/q)$. From this it is clear which values of x may enter the conditional congruences $b \equiv ax \pmod q$ of classes A and C; they are those x for which x^2+1 is a quadratic residue of q. ($u \not\equiv 0 \pmod q$). Conversely, for primes $p = a^2 + b^2$ and $\pm q \equiv 1 \pmod 4$ let the following congruence hold: $b \equiv ax \pmod q$ where x^2+1 is a quadratic residue of q; then from $p \equiv a^2(x^2+1) \pmod q$ we have $(p/q) = (\pm q/p) = 1$ i.e. $\pm q$ belongs to A or C modulo p; the symbol $((k^2+1)/q)$ defines to which of these classes it belongs, where k is a solution of $2x \equiv \mathrm{k} - 1/k \pmod q$. Therefore, whether $\pm q$ belongs to A or C de-

pends finally only on the value of x in the congruence $b \equiv ax \pmod q$ (theorem 1). It remains to determine the number of conditional congruences in classes A and C i.e. to prove theorem 5. Let us make k run through all numbers $1, 2, \ldots, q-1$, apart from the roots of the congruence $k^2+1 \equiv 0 \pmod q$, where of two values k and $-1/k$ we shall always take one only; then the formula $x \equiv \frac{1}{2}(k-1/k) \pmod q$ does, by above, give all the values x which enter into conditional congruences $b \equiv ax$ of classes A and C, and each occurs once only. Adjoining the congruence $a \equiv 0 \pmod q$, we may say that both classes A and C contain exactly $\frac{1}{2}(q-(-1)^{\frac{1}{2}(q-1)})$ conditional congruences. To determine the number of such congruences for each class A, C we must give k in formula $x \equiv \frac{1}{2}(k-1/k)$ only such values for which k^2+1 is a quadratic residue of q, i.e. the values of the form $k \equiv \frac{1}{2}(u-1/u) \pmod q$. Thus, let $u_1, u_2, \ldots, u_\nu$ be all the numbers of a reduced system of residues modulo q, distinct from ± 1 and from the roots of the congruence $u^2+1 \equiv 0 \pmod q$, and not connected by relation $uu' \equiv -1 \pmod q$. Clearly, the number of them is $\nu = \frac{1}{2}(q-4-(-1)^{\frac{1}{2}(q-1)})$. Taking $k_i \equiv \frac{1}{2}(u_i - 1/u_i) \pmod q$ $(i = 1, 2, \ldots, \nu)$, we see that all k_i are distinct, $\not\equiv 0 \pmod q$, and $((k_i^2+1)/q) = 1$. Choose among k_i half: $k_1, k_2, \ldots, k_{\frac{1}{2}\nu}$ not connected by $k_i k_j \equiv -1 \pmod q$ and take $x_i \equiv \frac{1}{2}(k_i - 1/k_i) \pmod q$, $(i = 1, 2, \ldots, \frac{1}{2}\nu)$. Then the congruences $b \equiv ax_i$ are all the conditional congruences of class A for $(2/q) = 1$, and of class C for $(2/q) = -1$. Adjoining congruence $a \equiv 0 \pmod q$ we see that in one of the classes A or C there is $\frac{1}{2}\nu+1 = \frac{1}{4}(q-(-1)^{\frac{1}{2}(q-1)})$ conditional congruences, and consequently the same number is contained in the other class, q.e.d. Clearly, the above reasoning provides also a convenient method for practical evaluation of conditional congruences for a given q.

§ 4. Cubic residues, Gauss's method

In the study of cubic residues we first remain in the domain of ordinary integers, and it is sensible to consider only the prime moduli p of the form $6n+1$. For such a modulus, the congruence $x^3 \equiv 1 \pmod p$ has three roots $1, f, f^2$ where f, f^2 satisfy the congruence $x^2+x+1 \equiv 0 \pmod p$. Let us split numbers $1, 2, \ldots, p-1$ according to § 6, ch. 1 into three classes A_0, A_1, A_2, referring to each class A_i all the numbers c for which $c^{\frac{1}{3}(p-1)} \equiv f^i \pmod p$. Then A_0 consists

of cubic residues, A_1 and A_2 – of cubic non-residues modulo p. For the other root f^2 of congruence $x^2+x+1 \equiv 0 \pmod{p}$ the class A_0 remains unchanged, whilst the classes A_1 and A_2 interchange places. In § 8, ch. 2 it has been proved that for a prime $p \equiv 1 \pmod 3$ equation $p = l^2+3m^2$ has a single solution in integers l, m (without taking their signs into account). Noting that the form x^2-xy+y^2 is transformed into x^2+3y^2 by substitution $\left(\begin{smallmatrix}1 & 1\\ 0 & 2\end{smallmatrix}\right)$ and into itself by means of $\left(\begin{smallmatrix}1 & 0\\ 1 & -1\end{smallmatrix}\right)$, it is easy to find that equation $p = x^2-xy+y^2$ has 12 solutions in integers: $x = \varepsilon l+\eta m$, $y = 2\eta m$ ($\varepsilon = \pm 1$, $\eta = \pm 1$); $x = 2\varepsilon m$, $y = \eta l+\varepsilon m$ ($\varepsilon = \pm 1$, $\eta = \pm 1$); $x = \varepsilon l+\eta m$, $y = \varepsilon l-\eta m$($\varepsilon = \pm 1$, $\eta = \pm 1$). Among these solutions there are two (and only two) satisfying condition $x \equiv 1$, $y \equiv 0 \pmod 3$. Denoting by f any root of the congruence $f^2+f+1 \equiv 0 \pmod{p}$, we may select from two solutions x, y of $p = x^2-xy+y^2$ one completely defined solution $x = a$, $y = b$ for which $a \equiv 1$, $b \equiv 0 \pmod 3$, $a+bf \equiv 0 \pmod{p}$. The numbers a, b play the same part for cubic distribution modulo $6m+1$, which is played by numbers a, b in equation $p = 4n+1 = a^2+b^2$ for biquadratic distribution.

Determining by examples when a given number q belongs to a class A_0, A_1 or A_2 to moduli $p = a^2-ab+b^2$, we see that it is defined by conditional congruences of the form $a \equiv 0$, $b \equiv ax \pmod{q}$, which are analogous to those of the previous section. These congruences express the cubic reciprocity law, and their complete proof is obtained only after the introduction of complex numbers of the form $x+y\rho$ (x, y-rational numbers, $\rho = \frac{1}{2}(-1+\sqrt{-3})$). We only consider the cases $q = 2$, $q = 3$, when the problem is solved by means of ordinary arithmetic. In the first memoir on quadratic residues (see [20], p. 511), Gauss gives a remarkable method for determining to which class A, B, C or D 2 belongs. This method also leads to an interesting theorem on the expression of a prime $p = 4n+1$ as a sum of two squares (see the following section). We have not given the exposition of Gauss's method in the previous section, since the question of the biquadratic character of 2 was solved there by a different method. We shall demonstrate Gauss's method on the theory of cubic residues (see T. J. Stieltjes [80], vol. I, pp. 210–275). Let a_i, a_i', a_i'', ... be all numbers of A_i ($i = 0, 1, 2$) to modulus $p = 6m+1$; denote by (ij) the number of $a_i, a_i', \ldots$, such that a_i+1, $a_i'+1$, ... belong to class A_j and let us determine nine quantities $(ij)(i, j = 0, 1, 2)$. Noting that α and

$-\alpha$ belong to the same class, we see that (ij) is the number of solutions of congruence $\alpha_i+\alpha_j+1 \equiv 0 \pmod p$ in numbers α_i, α_j of classes A_i, A_j, where two solutions (α_i, α_j) and (α_i', α_j') are considered the same only if $\alpha_i = \alpha_i'$, $\alpha_j \equiv \alpha_j' \pmod p$. Therefore, $(01) = (10)$, $(02) = (20)$, $(12) = (21)$. Noting further, that congruence $\alpha_0+\alpha_1+1 \equiv 0$ divided by α_1 becomes $\alpha_2+1+\alpha_2' \equiv 0$ where $\alpha_2 \equiv \alpha_0/\alpha_1$ and $\alpha_2' \equiv 1/\alpha_1$ belong to A_2 and, conversely, congruence $\alpha_2+1+\alpha_2' \equiv 0$ divided by α_2' becomes the original congruence we find $(01) = (22)$, and, similarly, $(02) = (11)$. These relations show that there are only four distinct values of $(\mu\nu)(\mu, \nu = 0, 1, 2)$. $(00) = i$, $(01) = (10) = (22) = j$, $(02) = (20) = (11) = h$, $(12) = (21) = k$. Since -1 belongs to A_0, the $\frac{1}{3}(p-1) = 2m$ quantities $a_\mu+1$, $a_\mu'+1$, ... $(a_\mu, a_\mu', \ldots$ are all numbers of $A_\mu)$, contain 0 only if $\mu = 0$. Consequently, $(00)+(01)+(02) = 2m-1$ and $(10)+(11)+(12) = 2m$. These relations allow us to express two of four values i, j, h, k, say, i, j, in terms of the other two h, k:

$$i = k-1, \quad j = 2m-h-k. \tag{13}$$

One more relation between i, j, h, k may be obtained on considering the congruence $\alpha_0+\alpha_1+\alpha_2+1 \equiv 0 \pmod p$ and on defining the number of its solutions in numbers α_0, α_1, α_2 of classes A_0, A_1, A_2 in two ways. In order to obtain the number of solutions for a given α_0, assume first that $\alpha_0+1 \equiv \alpha$ belongs to class A_0. The number of solutions of $\alpha_1+\alpha_2+\alpha \equiv 0$ for a given α does, clearly, coincide with the number of solutions of $\alpha_1'+\alpha_2'+1 \equiv 0$ in numbers α_1', α_2' of classes A_1, A_2 i.e. it is equal to (12). If α_0 is such that $\alpha_1+1 \equiv \beta$ belongs to A_1, then the number of solutions of $\alpha_1+\alpha_2+\beta \equiv 0$ for a given β is equal to (01); if, finally, $\alpha_0+1 \equiv \gamma$ belongs to A_2, then the number of solutions of $\alpha_1+\alpha_2+\gamma \equiv 0$ for a given γ is equal to (20). But since among numbers α_0+1 (α_0 are all the numbers of A_0 apart from -1), there are (00), (01), (02) numbers belonging to classes A_0, A_1, A_2 respectively, we conclude that $N = (00)(12)+(01)(01)+(02)(20) = ik+j^2+h^2$.

On performing a similar reasoning with α_1, i.e. on defining first the number of solutions of congruence $\alpha_0+\alpha_1+\alpha_2+1 \equiv 0$ for a given α_1, and then summing over all α_1, we obtain for N a different expression

$$N = jh+hk+kj.$$

Comparing this expression with the previous one, introducing in stead of i, j their expressions (13), and simplifying we obtain

$$3h^2+3hk+3k^2-6mh-(6m+1)k+4m^2 = 0. \tag{14}$$

To solve this indeterminate equation in two variables h, k we introduce instead of h, k integers X, Y defined by

$$h = \frac{6m-1+X}{9}, \quad k = \frac{6m+2+Y}{9} \tag{15}$$

after which equation (14) becomes $X^2+XY+Y^2 = 3(6m+1) = 3p$. From (15) it is clear that $(2X+Y)/9 = M$ is an integer; taking also $Y = L$ we find for L, M equation $L^2+27M^2 = 4p$. Apart from this equation L, M satisfy some congruences. One of them is $L \equiv 1 \pmod 3$. To obtain the other, consider the sum $S = \sum_{z=1}^{p-1}(z^3+1)^{\frac{1}{3}(p-1)}$. Recalling that $1^k+2^k+\ldots+(p-1)^k \equiv -1 \pmod p$ if k is divisible by $p-1$ and $\equiv 0 \pmod p$ otherwise (§ 7, ch. 1), we find

$$S \equiv -2 \pmod p.$$

Noting, on the other hand, that $S \equiv 3\sum(\alpha+1)^{\frac{1}{3}(p-1)} \pmod p$ where the summation is performed over all numbers of class A_0, we obtain

$$S \equiv 3(00)+3f(01)+3f^2(02) \pmod p,$$

where f is the root of the congruence $f^2+f+1 \equiv 0 \pmod p$ determining the distribution into classes A_0, A_1, A_2. Thus, we obtain $3i+3fj+3f^2h+2 \equiv 0 \pmod p$. Substituting here expressions for i, j, h through L, M (from (13), (15)):

$$i = \frac{p-8+L}{9}, \quad j = \frac{2p-4-9M-L}{18}, \quad h = \frac{2p-4+9M-L}{18},$$

$$k = \frac{p+1+L}{9},$$

and simplifying, we obtain

$$L+3M(f^2-f) \equiv 0 \pmod p.$$

Finally, taking $L = b-2a$, $3M = b$, we find that integers a, b satisfy

$$p = a^2-ab+b^2, \; a \equiv 1, \; b \equiv 0 \pmod 3, \; a+bf \equiv 0 \pmod p. \tag{16}$$

These conditions, according to the beginning of this section, com-

pletely determine integers a and b. Expressing i, j, h, k in terms of a, b we obtain, finally

$$\begin{aligned} i &= \tfrac{1}{9}(p-8+b-2a), \quad j = \tfrac{1}{9}(p-2-a-2b), \\ h &= \tfrac{1}{9}(p-2+a+b), \quad k = \tfrac{1}{9}(p+1+b-2a). \end{aligned} \tag{17}$$

In order to determine when 2 and 3 belong to classes A_0, A_1, A_2 moulo p, let us note that the number $(\mu\mu)$ of solutions of congruence $a_\mu + a'_\mu + 1 \equiv 0 \pmod p$ (a_μ, a'_μ belong to class A_μ, $\mu = 0, 1, 2$) is odd if and only if $a_\mu \equiv a'_\mu \equiv -\frac{1}{2}$ belongs to A_μ, i.e. when 2 belongs to $A_{3-\mu}$.

From (17) we find $(00) = i \equiv b+1$, $(11) = h \equiv a+b+1$, $(22) = j \equiv a+1 \pmod 2$ which gives the following theorem: 2 *belongs to* A_0 *modulo* p *when* b *is even, to* A_1 *when* a *is even, and to* A_2 *when* $a+b$ *is even, where* a, b *are defined for a prime* p *by* (16).

Let $\beta, \beta', \beta'', \ldots$ and $\gamma, \gamma', \gamma'', \ldots$ be all the numbers of classes A_1 and A_2; since all these numbers, and only they, are the roots of congruences $x^{\frac{1}{3}(p-1)} \equiv f$ and $x^{\frac{1}{3}(p-1)} \equiv f^2 \pmod p$ we have, by § 5, ch. 1

$$\begin{aligned} x^{\frac{1}{3}(p-1)} - f &\equiv (x-\beta)(x-\beta')(x-\beta'')\ldots, \\ x^{\frac{1}{3}(p-1)} - f^2 &\equiv (x-\gamma)(x-\gamma')(x-\gamma'')\ldots \pmod p. \end{aligned}$$

Taking $x = -1$, we find

$$\begin{aligned} 1 - f &\equiv (1+\beta)(1+\beta')\ldots, \\ 1 - f^2 &\equiv (1+\gamma)(1+\gamma')\ldots \pmod p. \end{aligned}$$

Raising these congruences to power $\frac{1}{3}(p-1)$ and remembering definition of $(\mu\nu)$, we obtain $(1-f)^{\frac{1}{3}(p-1)} \equiv f^{(11)+2(12)}$, $(1-f^2)^{\frac{1}{3}(p-1)} \equiv f^{(12)+2(22)} \pmod p$. Multiplying these congruences and noting that $(1-f)(1-f^2) \equiv 3$ we find $3^{\frac{1}{3}(p-1)} \equiv f^{(11)+2(22)} \pmod p$. But $(11) + 2(22) = h + 2j = \frac{1}{3}(p-1) + \frac{1}{3}(a-1) - \frac{1}{3}b$; From (16) we deduce $p \equiv a^2 - ab \pmod 9$, $\frac{1}{3}(p-1) \equiv \frac{1}{3}(a^2-1) - \frac{1}{3}ab \equiv -\frac{1}{3}(a-1) + (\frac{2}{3}b)$ and $h + 2j \equiv \frac{1}{3}b \pmod 3$. We obtain the following theorem: *if* a, b *are defined by conditions* (16), *then* 3 *belongs to classes* A_0, A_1, A_2 *modulo* p *if* $\frac{1}{3}b \equiv 0, 1, 2$ (*mod* 3) *respectively*.

§ 5. Theorem on the residue of a in the decomposition $p = a^2 + 4b^2$

Gauss's method of determining of the biquadratic character of 2 leads at the same time to a remarkable property of a decomposition

of a prime $p = 4n+1$ into a sum of two squares. This property may be formulated as follows: *if a prime* $p = 4n+1$ *is represented by a sum of two squares* $p = a^2+4b^2$ *where the sign of* a *is so chosen that* $a \equiv 1 \pmod 4$, *then* a *is the least absolute residue of the expression* $\frac{1}{2}(2n(2n-1)\dots(n+1))/(1\cdot 2\cdot\cdots n)$ *modulo* p (Gauss [20], p. 531). In previous section we have described Gauss's method for the case of cubic residues, hence we can obtain a similar theorem for the decomposition $4p = L^2+27M^2$. Note first that from the reasonings of the previous section concerning the form x^2-xy+y^2 it is easy to deduce that for a prime $p = 6m+1$ equation $4p = L^2+27M^2$ has a single solution in integers L, M apart from their signs. Consider the sum $S = \sum_{z=1}^{p-1}(z^3+1)^{\frac{1}{3}(p-1)}$; expressing every term by binomial expansion, we have

$$S \equiv -2-\frac{2m(2m-1)\dots(m+1)}{1\cdot 2\cdot 3\cdot\cdots m} \pmod p.$$

where $m = \frac{1}{3}(p-1)$. On the other hand, proceeding similarly to the previous section, we find

$$S \equiv 3(00)+3(01)f^2+3(02)f \pmod p.$$

Comparing both expressions for S and using expressions of $(00) = i$, $(01) = j$, $(02) = h$ in terms of L, M from the previous section, we obtain

$$3i+3jf^2+3hf+2 \equiv \tfrac{1}{2}L+\tfrac{3}{2}M(f-f^2)$$
$$\equiv -\frac{2m(2m-1)\dots(m+1)}{1\cdot 2\cdot 3\cdot\cdots m} \pmod p.$$

But for L and M we have found the following congruence

$$\tfrac{1}{2}L+\tfrac{3}{2}M(f^2-f) \equiv 0 \pmod p.$$

Adding these two congruences and remembering that for L defined as above, we have $L \equiv 1 \pmod 3$, we can formulate the following theorem: *let* $p = 3m+1$ *be a prime, and let the sign of* L *in equation* $4p = L^2+27M^2$ *be chosen by condition* $L \equiv 1 \pmod 3$; *then* L *is the least absolute residue of* $-(2m(2m-1)\dots(m+1))/(1\cdot 2\cdot 3\cdot\cdots m)$ *modulo* p.

Notes to chapter 3

§ 2. Concerning the distribution of power residues the following interesting theorem by Davenport [10] (1932) should be noted: *If $l > 0$ is an integer, and p is a prime $p \equiv 1 \pmod{l}$, $p > 100\, l^{12}$ then in the sequence* 1, 2, . . ., $p-1$ *there exist three consecutive residues of degree l modulo p.* In another paper 'On the distribution of quadratic residues (mod p)' [11] Davenport gives* approximations to sums of the form $\varphi_f = \sum_{x=0}^{p-1}(f(x)/p)$ where $f(x)$ is an integral polynomial whose leading coefficient is not divisible by a prime p (so that φ_f is the difference between the number of quadratic residues and non-residues modulo p in the sequence of numbers $f(0), f(1), \ldots, f(p-1)$). For example, if $f(x)$* is a polynomial of 7th degree, it is shown that φ_f is a quantity of order $p^{19/20}$. The method in the above papers is approximations by means of finite trigonometrical sums.

§ 3–4. In his second memoir on quadratic residues (see [20], p. 534) Gauss was the first to introduce *complex numbers* into the domain of arithmetic, when he studied numbers of the form $m+ni$ where $i = \sqrt{-1}$ and m, n are ordinary rational numbers. Gauss called $m+ni$ a *complex integer* if m, n are ordinary integers. The integer $N(\omega) = m^2+n^2$ is called the *norm* of a complex integer $\omega = m+ni$. If for two complex integers ω and $\zeta \neq 0$ the ratio ω/ζ is also an integer, it is said that ω is divisible by ζ. Integers ε of norm 1 (there exist four such: $\varepsilon = \pm 1, \pm i$) are called *units* they are divisors of every complex integer. Two integers ω and $\omega\varepsilon$ which differ only by a unit factor are called *associates*. An integer $\omega \neq \varepsilon$ is called a *prime* if it has no other divisors apart from numbers associate to it and units. Introducing these definitions Gauss proves that in the domain of complex integers the greatest common divisor of two integers may be found by means of an algorithm very similar to Euclidean algorithm, which results in the main theorem: *every integer ω may be represented in the form $\varepsilon\pi_1^{e_1}\pi_2^{e_2}\ldots$ where ε is a unit, $\pi_1, \pi_2, \ldots$ are distinct (i.e. non-associate) primes and $e_1, e_2, \ldots$ are positive powers. This factorisation is unique, i.e. every other factorisation of ω may be written as $\varepsilon'\pi_1'^{e_1}\pi_2'^{e_2}\ldots$ where the prime factors $\pi_1', \pi_2', \ldots$ are associates of $\pi_1, \pi_2, \ldots$ respectively.* The *primes* in the domain of complex numbers are as follows: 1) all

* Modell gave results for polynomials of smaller degree. The number of solutions of some congruences in two variables, Math. Z. 37 (1933).

ordinary primes p of the form $4n+3$ remain prime in the domain of numbers 2) every prime p of the form $4n+1$ does, by the Fermat theorem (§ 8, ch. 2) decompose uniquely into a sum of two squares a^2+b^2, and therefore $p = (a+ib)(a-ib)$; the factors $a+ib$ and $a-ib$ are clearly non-associate primes. Thus, an ordinary prime of the form $p = 4n+1$ is a composite number in the domain of complex numbers, whose two prime factors are $a+ib$ and $a-ib$. 3) $2 = -i(1+i)^2$ is an associate of the square of a prime $1+i$. After this, Gauss establishes the concept of congruences and theorems for complex numbers similar to Fermat and Euler theorems (§ 4, ch. 1). If ω is an *odd* complex number (i.e. not divisible by a prime $1+i$) then among four numbers $\varepsilon\omega$ associate to it, there exists one and only one congruent to a unity modulo $2+2i$. Such number is called *primary*. Let π be an odd prime complex number; all complex integers split into $N(\pi)$ distinct classes modulo π. Taking in each class one representative, we obtain a *complete system of residues modulo* π. Omitting in this system numbers $\equiv 0 \pmod{\pi}$ we obtain a *reduced* system of residues modulo π, consisting of $N(\pi)-1$ elements. For every element α of a reduced system of residues the following congruence holds

$$\alpha^{\frac{1}{4}(N(\pi)-1)} \equiv i^k \pmod{\pi}, \tag{18}$$

where index k is equal to 0, 1, 2 or 3. Corresponding to the values of the index, all the elements of a reduced system of residues modulo π split evenly into four classes, where numbers α for which $k = 0$ (and only they) are biquadratic residues modulo π. Introducing biquadratic symbol $(\alpha/\pi)_4 = i^k$ (see congruence (18)), we find that it possesses the properties of the ordinary Legendre symbol (§ 8, ch. 1). Finally, for two relatively prime complex numbers α and ω (of which the second one is odd) a generalised biquadratic symbol is introduced (similar to Jacobi symbol) assuming for the factorisation $\omega = \varepsilon\pi_1^{e_1}\pi_2^{e_2}\ldots$ into prime factors the corresponding symbol $(\alpha/\omega)_4 = (\alpha/\pi_1)_4^{e_1}(\alpha/\pi^2)_4^{e_2}\ldots$. We can now formulate the biquadratic reciprocity law: *if* ω *and* ζ *are two relatively prime primary complex numbers, then* $(\omega/\zeta)_4 = (-1)^{\frac{1}{4}(N(\omega)-1)\cdot\frac{1}{4}(N(\zeta)-1)}(\zeta/\omega)_4$.

The second memoir of Gauss on biquadratic residues ends with the formulation of this theorem (in a slightly different form) and with the proof of the theorems on biquadratic character of number $1+i$. The proof of the reciprocity law, found by him after many years of

hard work, Gauss intended to give in his third memoir on biquadratic residues which, however, never came out. One can guess the outline of the proof (which seems to be based on the geometrical interpretation of a lemma on biquadratic residues, similar to Gauss's lemma given in § 8, ch. 1) from the fragments of Gauss's manuscripts published after his death in the second volume of his collected works (see [19], pp.313–385). A strict rigorous proof of the biquadratic law of reciprocity in the same way as Gauss intended to give it, is given by Busche in the memoir 'Arithmetische Beweis des Reciprocitätsgesetzes für die biquadratischen Reste' [7]. In his latest paper (1912) Busche considerably simplified this proof and presented it in a visual geometrical form.

For a complete grasp of the theory of *cubic* residues, it is necessary to introduce complex integers of the form $m+\rho n$ (m, n – rational integers, $\rho = \frac{1}{2}(-1+\sqrt{-3})$ is a cubic root of unity). Since these numbers are quite similar to Gauss's numbers $m+ni$ we give only a brief account on them, which is necessary for formulation of the cubic reciprocity law. In the domain of numbers $m+n\rho$ the number $3 = -\rho^2(1-\rho)^2$ is associated with the square of a prime $1-\rho$. From six numbers $\pm\omega$, $\pm\rho\omega$, $\pm\rho^2\omega$ associated to a given integer ω, not divisible by $1-\rho$, there exists only one congruent to unity modulo 3, such number is, again, called *primary*. If π is a given prime modulus distinct from $1-\rho$, then for every complex intger α, not divisible by π, we have $\alpha^{\frac{1}{3}(N(\pi)-1)} \equiv \rho^k \pmod{\pi}$ where $k = 0, 1, 2$ and $N(\pi) > 0$ is a rational integer equal to the product of π and a complex number conjugate to it. Numbers α for which $k = 0$ in the above congruence (and only these) are cubic residues modulo π. Using the above congruence, we define the cubic symbol as $(\alpha/\pi)_3 = \rho^k$. Defining, similarly to the above, a general cubic symbol, we may formulate the cubic reciprocity law as follows: *let* ω, ζ *be two relatively prime primary complex numbers, then we always have* $(\omega/\zeta)_3 = (\zeta/\omega)_3$. This theorem was proved by the method of the division of the circle of Jacobi and Eisenstein. Its arithmetical (in fact, arithmetical-geometrical) proof, similar to the above Busche proof, was given by A. M. Juravsky [32].

Conditional congruences, given in § 3, defining when a given number belongs to a particular class to a given modulus, are in close connection with the biquadratic reciprocity law.This connection (and the same for cubic residues) was investigated by Stieltjes in his mem-

oir 'Contribution à la théorie des résidus cubiques et biquadratiques' (see [80], vol. I. pp. 210–275). The exposition of the theory of Gaussian numbers can also be found in a textbook by Dirichlet [14], suppl. XI. The complex numbers $m+ni$ and $m+n\rho$ described there resulted in a vast generalisation of ordinary arithmetic given in papers by Kummer, Kronecker, Dedekind and many later authors, which now forms a vast theory of *algebraic integers*. Finally, the author of the present monograph has proved that the domain of Hamilton's *quaternions* $a+bi+cj+dk$ has the same simple arithmetic as the domain of Gaussian complex numbers (see Venkov [95]).

§ 5. Theorems, similar to this section exist also for the representation of primes in form x^2+2y^2, x^2+3y^2, x^2+7y^2. See Jacobi, 'Über die Kreistheilung und ihre Anwendung auf die Zahlentheorie' ([31] pp. 254–274) and Stieltjes, 'sur la décomposition quadratique de nombres premiers de la forme $3n+1$' (see [80], vol. I). Another method for the proof of the theorems given in the text was given by Eisenstein (using the theory of elliptic functions).

4. GAUSS'S THEORY OF QUADRATIC FORMS

§ 1. On the representation of an integer by a binary quadratic form

In 'Disquisitiones Arithmeticae', Gauss has given the theory of quadratic forms, which collects together all results of Fermat, Euler and Lagrange, and includes several very important discoveries by Gauss himself. The present chapter is concerned with this theory of quadratic forms.

In § 3 ch. II were given the principal definitions concerning binary quadratic forms, in particular, the definition of *equivalence* of two forms f and f'. Gauss distinguishes between *proper* and *improper* equivalence, which occurs when the determinant of the integral substitution transforming f into f' is equal to $+1$ or -1. The main problem in the theory of binary forms is the following: Let $f = f = ax^2+2bxy+cy^2$ be a given form with integral coefficients a, b, c, and let m be an integer; find all the representations of integer m by means of form f, i.e. find all solutions of indeterminate equation of second degree in two variables (see § 7 below). The latter problem can first be restricted to finding the proper representations, i.e. representations in which x and y are relatively prime. (cf. § 8, ch. II). Thus, let $f=ax^2+2bcay+xy^2$ be an integral quadratic form (i.e. a, b, c are integers), and let $m \neq 0$ be an integer. Let $x = \alpha$, $y = \gamma$ be a proper representation of m by form f. Take a pair of integers β, δ, satisfying $\alpha\delta-\beta\gamma = 1$, and transform f by substitution $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ into a properly equivalent form f'. The first coefficient of f' is $a\alpha^2+2b\alpha\gamma+$ $+c\gamma^2 = m$; taking $f' = mx'^2+2nx'y'+ly'^2 = (m, n, l)$ and denoting by d the determinant of forms f and f', we obtain the remaining coefficients n, l of f' as follows:

$$n = a\alpha\beta+b(\alpha\delta+\beta\gamma)+c\gamma\delta, \quad n^2-ml = d. \tag{1}$$

The second formula above shows that $n^2 \equiv d \pmod{m}$, i.e. that

d is a quadratic residue of m. Thus, for a proper representation of m by form f to be possible, it is necessary that d is a quadratic residue of m. Taking instead of β, δ another pair of integers β', δ' satisfying equation $\alpha\delta-\beta\gamma = 1$, we have $\beta' = \beta+\alpha t$, $\delta' = \delta+\gamma t$ (t an integer); number n' constructed for new integers β', δ' (see (1)) has value $n' = (a\alpha+b\gamma)\beta'+(b\alpha+c\gamma)\delta' = n+mt$, i.e. $n' \equiv n \pmod m$. Thus, if we pass from β, δ to another solution of $\alpha\delta-\beta\gamma = 1$, the middle coefficient n of form $f' = (m, n, l)$ remains in the same class modulo m, which is the class of numbers n satisfying the congruence $n^2 \equiv d \pmod m$, and is completely defined by a primitive representation α, γ of number m by form f. The representation α, γ is said to belong to the root n of congruence $n^2 \equiv d \pmod m$. Moreover, when t runs through all integers from $-\infty$ to $+\infty$, the expressions $\beta' = \beta+\alpha t$, $\delta' = \delta+\gamma t$ give *all* solutions of equation $\alpha\delta-\beta\gamma = 1$ in integers β, δ, and the numbers $n' = n+mt$ run through *all* the integers of the above class modulo m, taking each value once only. Defining β, δ from the first formula of (1) and from $\alpha\delta-\beta\gamma = 1$, we obtain $n\alpha-b\alpha-c\gamma = m\beta$, $n\gamma+a\alpha+b\gamma = m\delta$, or $n\alpha \equiv b\alpha+c\gamma$, $-n\gamma \equiv a\alpha+b \pmod m$. Since α and γ are relatively prime, these congruences, as well as (1), may serve to determine the residue class modulo m to which the representation α, γ belongs. Conversely, if a, b, c, n and $m \neq 0$ are given integers, and there exists a pair of numbers α, γ satisfying the conditions

$$a\alpha^2+2b\alpha\gamma+c\gamma^2 = m, \quad a\alpha+(b+n)\gamma \equiv 0, \quad (b-n)\alpha+c\gamma \equiv 0 \pmod m, \tag{2}$$

then α, γ is a proper representation of m by form $f = (a, b, c)$ which belongs to a root n of congruence $n^2 \equiv d \pmod m$. In fact, writing congruences (2) in the form of equations with $m\delta$ and $-m\beta$ in their right hand sides (β, δ are integers), we deduce from these equations first $m = m(\alpha\delta-\beta\gamma)$ i.e. $\alpha\delta-\beta\gamma = 1$ (so that $(\alpha, \gamma) = 1$), and then obtain (1); q.e.d. We shall use this proposition when considering the composition of forms in § 10.

The above exposition provides the method for obtaining all proper representations of a number m by a form f. Since the congruence $n^2 \equiv d \pmod m$ has to be solvable, denote by n', n'', n''', ... all its solutions, incongruent modulo m. Define for every $n^{(i)}$ an integer $l^{(i)}$ by formula $l^{(i)} = ((n^{(i)})^2-d)/m$ and construct the forms

(m, n', l'), (m, n'', l'') of determinant d. Select from these forms those which are properly equivalent to the given form f, and, if $f' = (m,n',l')$ is one such form, find all the substitutions $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$, $(\alpha\delta - \beta\gamma) = 1$, transforming f into f'. Then the pairs α, γ in these substitutions give all possible representations of m by form f, which belong to the root n'. Proceed similarly with the remaining forms (m, n'', l'') (m, n''', l'''),.... equivalent to f. This leads us to the two following questions on the equivalence of forms, the solution of which completely answers the problem of finding all the proper representations of a given number by a given form: 1). To find whether two integral forms f, f' of the same determinant are properly equivalent. 2) If f and f' are equivalent, find all integral substitutions of determinant 1 transforming f into f'. Solution of these two problems follows shortly. It is easy to see that the definition of the present section of a proper representation which appertains to the root of a congruence $n^2 \equiv d \pmod{m}$ is a generalisation of the same definition which was given earlier for a particular case. (§ 8, ch. II).

§ 2. Transformation of a binary form into itself

The solution which will be given in §§ 3, 5, 6 for the first question on equivalence posed in the last section (to find whether two given forms f and f' are equivalent) provides, in the case of equivalence of f and f', a substitution transforming f into f'. Therefore, the second question on equivalence may be restated as follows: given a substitution S_0 of determinant 1, which transforms form f into f'; find all other substitutions S of the same kind. Clearly, if T is a substitution which transforms form f into itself, then the product substitution TS_0 of T by S_0 is a transformation of type S. (§ 3, ch. II). If $S_0 = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$, then substitution $S_0^{-1} = \begin{pmatrix} \delta & -\beta \\ -\gamma & \alpha \end{pmatrix}$ which is called the *inverse* of S transforms f' into f. The products $S_0 S^{-1}$ and $S_0^{-1} S_0$ are equal to the *unitary* substitution $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ which will be denoted by 1. If S is a substitution transforming f into f' then SS_0^{-1} transforms f into itself and therefore belongs to substitutions T, hence $S = TS_0$. Therefore,

substitutions S coincide with all substitutions TS_0 and our problem becomes the following: find all integral substitutions T of determinant 1 which transform a given form f into itself. Take $f = ax^2+2bxy+cy^2$ where a, b, c are integers, $a \neq 0$ (the assumption necessary only for the case when determinant $d = b^2-ac$ is a perfect square), and assume $T = \begin{pmatrix} \lambda & \mu \\ \nu & \rho \end{pmatrix}$. The required numbers λ, μ, ν, ρ are defined by the conditions:

$$\begin{gathered} \lambda\rho-\mu\nu = 1, \quad a\lambda^2+2b\lambda\nu+c\nu^2 = a \\ a\lambda\mu+b(\lambda\rho+\mu\nu)+c\nu\rho = b \end{gathered} \tag{3}$$

which are necessary and sufficient for T to transform f into itself. The first and the third of the above formulae give $a\lambda\mu+2b\mu\nu+c\nu\rho=0$, which together with the second formula (3) gives $c\nu = -a\mu = 2b\nu = a(\rho-\lambda)$. Let $\sigma > 0$ be the greatest common divisor of a, $2b$, c. Since $a \neq 0$, we may assume $\nu = (a/\sigma)u$ (u is rational) and then the previous formulae give $\mu = -(c/\sigma)u$, $\rho-\lambda = (2b/\sigma)u$, from which, since a/σ, $2b/\sigma$, c/σ have no common factor, we conclude that u is an integer. Substituting the values of ν, μ obtained above into the first formula (3), we find $\lambda\rho = (ac/\sigma^2)u^2+1$ and $(\rho+\lambda)^2 = (\rho-\lambda)^2+4\lambda\rho = (4d/\sigma^2)u^2+4$ from which it is clear that $\frac{1}{2}\sigma(\rho+\lambda) = t$ is an integer satisfying equations $t^2-du^2 = \sigma^2$. Thus, we find the following formulae for coefficients of T:

$$\lambda = \frac{t-bu}{\sigma}, \quad \mu = -\frac{cu}{\sigma}, \quad \nu = \frac{au}{\sigma}, \quad \rho = \frac{t+bu}{\sigma}. \tag{4}$$

Conversely, we can easily see (L. Dirichlet [14], § 62), that for integers t, u satisfying equation $t^2-du^2 = \sigma^2$ numbers (4) are integers, satisfying (3). Thus, *if* $f = (a, b, c)$ $(a \neq 0)$ *is an integral form with determinant* d, *then each substitution* T *with determinant* $+1$, *transforming* f *into itself, is obtained once only from*

$$T = \begin{pmatrix} \dfrac{t-bu}{\sigma} & -\dfrac{cu}{\sigma} \\ \dfrac{au}{\sigma} & \dfrac{t+bu}{\sigma} \end{pmatrix} \tag{5}$$

when t, u *run through all solutions of the Pellian equation* $t^2-du^2 = \sigma^2$ *where* $\sigma > 0$ *is the greatest common divisor of* a, $2b$, c.

Let us note that $4d = 4b^2 - 4ac \equiv 0 \pmod{\sigma^2}$. Moreover, if $2b/\sigma$ is even, then σ is the greatest common divisor of a, b, c and $d \equiv 0 \pmod{\sigma^2}$. If $2b/\sigma$ is odd, then $4d \equiv \sigma^2(2b/\sigma)^2 \equiv \sigma^2 \pmod{4\sigma^2}$ i.e. $4d/\sigma^2$ is an integer of the form $4k+1$. By the previous reasoning, the transformations of f into another form f', are of the form TS_0, where $S_0 = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ is one of such substitutions. Combining this with the results of the previous section concerning the proper representations of m by a form $f = (a, b, c)$, we obtain the following result: if there exists a proper representation α, γ of a number m by a form f, which belongs to a root of congruence $n^2 \equiv d \pmod{m}$, then all the remaining representations α', γ', appertaining to the same root, are obtained from

$$\alpha' = \frac{\alpha}{\sigma} t - \frac{b\alpha + c\gamma}{\sigma} u, \quad \gamma' = \frac{\gamma}{\sigma} t + \frac{\alpha a + b\gamma}{\sigma} u, \tag{6}$$

where t, u run through all solutions of the Pellian equation $t^2 - du^2 = \sigma^2$. Clearly, for $d < 0$ this equation has a finite number of solutions, namely: two solutions if $|4d/\sigma^2| > 4$, four solutions if $d/\sigma^2 = -1$, and six solutions if $4d/\sigma^2 = -3$. The same can be said for proper representations of a given number by a form which belong to a given root of the congruence $n^2 \equiv d \pmod{m}$, assuming, of course, that such representations of m by f exist. If d is distinct from zero and is a square of an integer, the Pellian equation has a finite number of solutions. Finally, for $d > 0$ and not equal to a square, it was shown in § 12 ch. II, that this equation has an infinite number of solutions, and we know how to find all these solutions for the case $d \equiv 0 \pmod{\sigma^2}$ when equation $t^2 - du^2 = \sigma^2$ is reduced to the form $t'^2 - d'u^2 = 1$ which was investigated in § 12, ch. II ($t' = t/\sigma$, $d' = d/\sigma^2$). Let us note that if we know one identical substitution $T = \begin{pmatrix} \lambda & \mu \\ \nu & \rho \end{pmatrix}$ transforming form f into itself, then by (4) we find at once a non-trivial solution of the Pellian equation $t^2 - du^2 = \sigma^2$; for example, we may take $t = \frac{1}{2}\sigma(\rho + \lambda)$, $u = \sigma\nu/a$. Therefore, if we have a method for determining substitutions T, this method provides all solutions of the Pellian equation (see below, § 5).

§ 3. Reduction of forms with a negative determinant

Returning to the first question on equivalence posed in § 1, we first consider the case of a negative determinant $d < 0$; in this case it suffices to consider only positive forms (i.e. forms with positive first and last coefficients). In § 3, ch. II we have proved that every positive form is properly equivalent to a *reduced* form, i.e. a form $f = (a, b, c)$ whose coefficients satisfy $|2b| \leqq a \leqq c$. Moreover, 1) if the coefficients of the original form are integers, then so are the coefficients a, b, c of the reduced form; 2) the algorithm of § 3, ch. II gives at the same time an integer substitution with determinant 1, transforming a given form into a reduced form. In § 3 ch. II we saw that from the conditions of reducibility $|2b| \leqq a \leqq c$ it follows that $a \leqq \sqrt{\frac{4}{3}|d|}$, from which $|b| \leqq \sqrt{\frac{1}{3}|d|}$. For a given d this inequality is satisfied only by a finite number of pairs of integers a, b, and for every pair a, b there exists no more than one integer value of c. Therefore, the number of reduced forms with a given negative determinant is finite; calling by a *class* the set of all forms properly equivalent to the same form (Gauss, D. A., art. 223), we may state the following theorem:

THEOREM 13. *For every determinant $d \neq 0$ the number of distinct classes is finite.*

The reasoning above proves the theorem only for the case $d < 0$; for the case $d > 0$ it will be proved later (§§ 5, 6). It may still be possible for two non-identical forms of determinant $d < 0$ to be properly equivalent. To find out whether this is so, take $f = (a, b, c)$, $f' = (a', b', c')$, $|2b| \leqq a \leqq c$, $|2b'| \leqq a' \leqq c'$, $b^2 - ac = b'^2 - a'c' = d$, ($a, b, c, a', b', c'$ are integers), and let f be transformed into f' by substitution $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$. We have

$$\begin{aligned} \alpha\delta - \beta\gamma = 1, \quad a' &= a\alpha^2 + 2b\alpha\gamma + c\gamma^2 \\ b' &= a\alpha\beta + b(\alpha\delta + \beta\gamma) + c\gamma\delta \end{aligned} \tag{7}$$

Clearly, we may assume $a' \leqq a$. The second equality (7) gives $aa' = (a\alpha + b\gamma)^2 - d\gamma^2$, and since $aa' \leqq \frac{4}{3}|d|$, we have $\gamma^2 \leqq 1$ and, consequently, $\gamma = 0$ or ± 1. If $\gamma = 0$ than $\alpha\delta = 1$, $\alpha = \delta = \pm 1$, $a' = a$ and $b' - b = a\alpha\beta$, i.e. $b' - b$ is divisible by a. But $|b| \leqq \frac{1}{2}a$, $|b'| \leqq \frac{1}{2}a$, hence $b' - b$ is equal either to zero, or to $\pm a$. If $b' - b = 0$,

then $c' = c$ and the forms f and f' are identical; if $b' - b = \pm a$ then $b' = -b \pm \frac{1}{2}a$ (so that a is even), $c' = c$ and forms f, f' are of the form $(a, -\frac{1}{2}a, c)$ and $(a, -\frac{1}{2}a, c)$. These forms are, in fact, equivalent, namely, the first is transformed into the second by means of substitution $\begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}$. In the case $\gamma = \pm 1$, the second formula (7) gives $a' = a\alpha^2 + 2b\alpha\gamma + c$ and, since we assume $a' \leqq a$, and consequently $a' \leqq c$, we have $a\alpha^2 + 2b\alpha\gamma \leqq 0$; but $|2b\alpha\gamma| = |2b\alpha| \leqq a\alpha^2$ and thus $a\alpha^2 + 2b\alpha\gamma = 0$, $a' = c$, $a = a'$. The first and the third formulae (7) give, further, $b' + b = a\alpha\beta + 2b\alpha\delta + c\gamma\delta = a\alpha\beta - a\alpha^2\gamma\delta + a\gamma\delta \equiv 0 \pmod{a}$ from which, similarly to the above, we deduce that either $b' + b = \pm a$, $b' = b = \pm \frac{1}{2}a$, $c' = c$ and forms f and f' are identical, or $b' + b = 0$, $c' = c = a' = a$ and f, f' are of the form (a, b, a) and $(a, -b, a)$. These forms are not identical for $b \neq 0$, and the first one is transformed into the second by means of substitution $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$.

There are no other cases of two non-identical reduced forms being equivalent. It is convenient to specify the conditions for reducibility in such a way, that the resulting reduced forms do not contain forms properly equivalent to each other. Using the above results this may be done as follows. Let us make coefficients a, b, c of form f satisfy one of the following conditions

$$1)\ |2b| < a < c, \quad 2)\ 0 \leqq 2b < a = c, \quad 3)\ 0 < 2b = a \leqq c. \quad (8)$$

Then we may say that every positive form of a given determinant is properly equivalent to one and only one of the forms of the types described above. From now on by a *reduced* positive form is understood to be only a form, whose coefficients satisfy (8).

Let f, f' be two integral forms of the same determinant $d < 0$. Using the algorithm of § 3, ch. II, we find substitutions S, S', of determinant 1, transforming f, f' into reduced forms f_0, f_0'. If $f_0 \neq f_0'$, then the forms f, f' are not properly equivalent; if $f_0 = f_0'$, then f, f' are equivalent transforms into f by substitution SS'^{-1}. This solves the first question posed in § 1 on the equivalence of the forms. Moreover, from § 2 follows a solution of the second question in the case $d < 0$. Therefore, for a negative determinant the question of finding the primitive (and, consequently, all) representations of a given number by a given form is solved completely.

§ 4. Forms of a positive determinant

Consider the forms of a positive determinant assuming in this section their coefficients to be real numbers. Moreover, we assume that the form $f = ax^2+2bxy+cy^2$ is zero only when x and y are both zeroes; then a and c are distinct from zero, and the roots of the equation $a+2bz+cz^2 = 0$ are real, distinct, and irrational. Let us call the root $\Omega = (-b-\sqrt{d})/c$ the first root, and the root $\omega = (-b+\sqrt{d}/c)$ – the second root of f. (L. Dirichlet [14], § 72), where $d = b^2-ac > 0$ is the determinant of f. If f is transformed into f' by substitution $\begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix}$ with determinant $\varepsilon = \alpha\delta-\beta\gamma = \pm 1$, then $f'\begin{pmatrix}\delta & -\beta\\ -\gamma & \alpha\end{pmatrix} = f$ and expressions $(\alpha\Omega-\gamma)/(\delta-\beta\Omega)$ and $(\alpha\omega-\gamma)/(\delta-\beta\omega)$ are ,clearly, equal to the roots of the form f'. Substituting $\Omega = (-b-\sqrt{d})/c$ into $(\alpha\Omega-\gamma)/(\delta-\beta\Omega)$ and on getting rid of $\sqrt{d}$ in the denominator, we find that $(\alpha\Omega-\gamma)/(\delta-\beta\Omega)$ is equal to the first root of f' for $\varepsilon = +1$, and to the second root of f' for $\varepsilon = -1$. Thus, if form f by substitution $\begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix}$ of determinant $+1$ is transformed into form f' with roots Ω', ω' then the corresponding roots of these forms are connected by relations

$$\Omega = \frac{\gamma+\delta\Omega'}{\alpha+\beta\Omega'}, \quad \omega = \frac{\gamma+\delta\omega'}{\alpha+\beta\omega'}.$$

A form f with roots Ω, ω is called *reduced* if $|\Omega| > 1$, $|\omega| < 1$, $\Omega\omega < 0$. This definition is very similar to the one given in § 10, ch. II for reduced quadratic irrationalities. Here we find, similarly, that for a reduced form $f = (a, b, c)$, $0 < b < \sqrt{d}$, $ac < 0$, $|a|$ and $|c|$ fall between $\sqrt{d}-b$ and $\sqrt{d}+b$, $\Omega a > 0$; conversely, a system of inequalities $0 < \sqrt{d}-b < |c| < \sqrt{d}+b$ or $0 < \sqrt{d}-b < |a| < \sqrt{d}+b$ characterises the reducibility of form f. *Every form with determinant $d > 0$ is properly equivalent to a reduced form.* Let f be a given form with roots Ω, ω. We develop Ω into a simple continued fraction $\Omega = [a_1, a_2, \ldots, a_n, \Omega_n](n = 1, 2, \ldots)$ where $\Omega_n > 1$ is a complete quotient, and define, for every n an irrational number ω_n from equation $\omega = [a_1, a_2, \ldots, a_n, \omega_n]$. ω_n cannot exceed one for every n, for then $\Omega = \omega$; consequently, there exists a number n for which $\omega_n < 1$ and then $\omega_{n+1} < 0$, $-1 < \omega_{n+2} < 0$, $-1 < \omega_{n+3} < 0, \ldots$. Thus, we

see that we may select an *even* number n such that in the equalities

$$\Omega = [a_1, a_2, \ldots, a_n, \Omega_n] = \frac{P_{n-1}+P_n\Omega_n}{Q_{n-1}+Q_n\Omega_n}, \quad \omega = \frac{P_{n-1}+P_n\omega_n}{Q_{n-1}+Q_n\omega_n}$$

we have $\Omega_n > 1$, $-1 < \omega_n < 0$ (P_n/Q_n denotes a convergent to fraction $[a_1, a_2, \ldots]$). Transforming f by means of substitution $\begin{pmatrix} Q_{n-1} & Q_n \\ P_{n-1} & P_n \end{pmatrix}$ of determinant 1, we obtain a form with roots Ω_n, ω_n, i.e. a reduced form, q.e.d.

Remembering the definition of *neighbouring* forms given in § 3, ch. II, we prove that for a reduced form there exists one and only one reduced form neighbouring on the right. Let f be transformed by $\begin{pmatrix} 0 & -1 \\ 1 & k \end{pmatrix}$ (k is an integer) into an neighbouring form $f' = (c, b', c')$. Denote by $\Omega, \omega, \Omega', \omega'$ the roots of the forms f, f'. Then $\Omega = -k - 1/\Omega'$, $\omega = -k - 1/\omega'$. If f and f' are reduced forms, then $|\Omega| > 1$, $|\Omega'| > 1$. It is clear from $\Omega = -k - 1/\Omega'$ that $k \neq 0$ and since $-k - 1/\Omega'$ has the same sign as $-k$, we have $k\Omega < 0$. Further, $a\Omega > 0$, $c\Omega' > 0$, consequently, $\Omega\Omega' < 0$ and $|\Omega| = |k| + 1/|\Omega'|$, so that $|k| = [|\Omega|]$. Conditions $|k| = [|\Omega|]$, $k\Omega < 0$ define integer k completely for a given form f; conversely, defining k by these conditions, and transforming f by substition $\begin{pmatrix} 0 & -1 \\ 1 & k \end{pmatrix}$ into form f' with roots Ω', ω' we easily find from relations $\Omega = -k - 1/\Omega'$, $\omega = -k - 1/\omega'$ that $|\Omega'| > 1$, $|\omega'| < 1$, $\Omega\Omega' < 0$, $\Omega\omega' > 0$, i.e. that f' is a reduced form. Noting that from $(a, b, c)\begin{pmatrix} 0 & -1 \\ 1 & k \end{pmatrix} = (c, b', a')$ follows $(a', b', c)\begin{pmatrix} 0 & -1 \\ 1 & k \end{pmatrix} = (c, b, a)$ and that the form (c, b, a) reduces simultaneously with (a, b, c), we find that for a given reduced form (a, b, c) there exists one and only one reduced left neighbouring form.

Let $f = (a, b, a_1)$ be a reduced form; let us find the reduced form $f_1 = (a_1, b_1, a_2)$ neighbouring to f on the right, and then a reduced form $f_2 = (a_2, b_2, a_3)$ neighbouring to f_1 on the right, etc.
We obtain a series of forms

$$\ldots (a_{-2}, b_{-2}, a_{-1}) \begin{pmatrix} 0 & -1 \\ 1 & k_{-2} \end{pmatrix} (a_{-1}, b_{-1}, a) \begin{pmatrix} 0 & -1 \\ 1 & k_{-1} \end{pmatrix}$$
$$(a, b, a_1) \begin{pmatrix} 0 & -1 \\ 1 & k \end{pmatrix} (a_1, b_1, a_2) \begin{pmatrix} 0 & -1 \\ 1 & k_1 \end{pmatrix} (a_2, b_2, a_3) \ldots \quad (9)$$

Since the roots of f are irrational, the above series continues indefinitely to the right and to the left; it is called the *period* of the form f (see A. A. Markov [54], p. 4) Denoting by Ω_n, ω_n the roots of the form $f_n = (a_n, b_n, a_{n+1})$, we have

$$\ldots, \Omega_{-2} = -k_{-2} - \frac{1}{\Omega_{-1}}, \quad \Omega_{-1} = -k_{-1} - \frac{1}{\Omega}, \tag{10}$$

$$\Omega = -k - \frac{1}{\Omega_1}, \quad \Omega_1 = -k_1 - \frac{1}{\Omega_2}, \ldots$$

$$\ldots, \omega_{-2} = -k_{-2} - \frac{1}{\omega_{-1}}, \quad \omega_{-1} = -k_{-1} - \frac{1}{\omega},$$

$$\omega = -k - \frac{1}{\omega_1}, \quad \omega_1 = -k_1 - \frac{1}{\omega_2}, \ldots \tag{11}$$

Denoting by l_i the absolute value of k_i, we obtain from the above relations the following developments of $|\Omega_n|$ and $1/|\omega_n|$ into continued fractions for all $n = 0, \pm 1, \pm 2, \ldots$.

$$|\Omega_n| = [l_n, l_{n+1}, l_{n+2}, \ldots], \quad \frac{1}{|\omega_n|} = [l_{n-1}, l_{n-2}, l_{n-3}, \ldots]. \tag{12}$$

Using the properties of reduced forms, it is not difficult to prove Korkine's previously formulated theorem (end § 3, ch. II), on the minimum of a form of a positive determinant d. Let $f = (a, b, a_1)$ be a given reduced form of determinant d; we construct the corresponding period (9) of reduced forms. Since the difference $\Omega_n - \omega_n$ of the roots of the form f_n is equal to $-2\sqrt{d}/a_{n+1}$ and these roots are of opposite signs, we obtain by (12)

$$\frac{2\sqrt{d}}{a_{n+1}} = |\Omega_n| + |\omega_n| = l_n + \cfrac{1}{l_{n+1} + \cfrac{1}{l_{n+2} + \ddots + \cfrac{1}{l_{n-1} + \cfrac{1}{l_{n-2} + \ddots}}}} \tag{13}$$

for every n. Let us show that n may be chosen in such a way that the expression on the right hand side of (13) is greater or equal to $\sqrt{5}$. In fact, consider a sequence of positive integers $\ldots, l_{-1}, l_0, l_1, l_2, \ldots$. If in this sequence there is at least one element greater or equal to 3,

e.g. l_i then we achieve our aim if we take $n = i$ in (13). If the sequence is composed exclusively of ones and two's and contains at least one two $l_i = 2$, say, then for $n = i$ the right hand side of (13) is greater than $2+\frac{1}{3}+\frac{1}{3} = 2.66\ldots > \sqrt{5} = 2.23\ldots$. Finally, if $l_i = 1$ for all l_i, then the right hand side of (13) is equal to $\sqrt{5}$ for every n. Therefore, there always exists n for which $|a_{n+1}| \leqq 2\sqrt{d}/\sqrt{5}$, and since a_{n+1} is equal to the value of form f for some integers x, y we see that for every reduced form f there exist integral values of x, y, not simultaneously zero, for which $|f| \leqq \sqrt{\frac{4}{5}d}$. This theorem is true not only for a reduced, but for any form of determinant d, since it has been proved that every form is equivalent to a reduced one. It has already been noted (§ 3, ch. II), that the limit $\sqrt{\frac{4}{5}}$ cannot be lowered since the form $\sqrt{\frac{4}{5}d}(x^2+xy-y^2)$ (and all the forms equivalent to it properly and improperly) cannot be made less than $\sqrt{\frac{4}{5}d}$ by means of integral values x, y not simultaneously zero. Assume now that the given form of determinant d is not equivalent to $\sqrt{\frac{4}{5}d}(x^2+xy-y^2)$. Transforming it into a reduced form f, and constructing period (9), we find that the sequence $\ldots, l_{-1}, l_0, l_1, \ldots$ cannot consist of ones only; after which, similarly to the above, we show, that n in (13) may be so chosen that the right hand side of (13) is greater or equal to $2\sqrt{2}$. We obtain the following theorem: *in every form f of determinant $d > 0$, not equivalent to $\sqrt{\frac{4}{5}d}(x^2+ay-y^2)$, the variables x, y may be given integer values, not simultaneously zero, such that $|f| \leqq \sqrt{\frac{1}{2}d}$*, where the limit is again a precise limit for the form $\sqrt{\frac{1}{2}d}(x^2-2xy-y^2)$ and the forms equivalent to it. Developing this theory further A. A. Markov obtained, in his dissertation, an infinite set of such limits, and found a remarkable relation between these limits and the solutions of an indeterminate equation $x^2+y^2+z^2 = 3xyz$ in integers x, y, z. (see notes to the present chapter).

Let us prove now that *it two reduced forms f and f' are properly equivalent, then one of them is contained in the period of the other.* Let f transform into f' by substitution $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$, $\alpha\delta-\beta\gamma = 1$. Since in passing from a reduced form to its neighbouring reduced form on the right or on the left the sign of the leading coefficient is changed, we may assume that in the forms $f = (a, b, a_1)$ and $f' = (a', b', a'_1)$ we have $a > 0$, $a' > 0$. Denoting then the roots of forms f and f' by Ω, ω and Ω', ω', we have

$$\Omega > 1, \quad \Omega' > 1, \quad -1 < \omega < 0, \quad -1 < \omega' < 0,$$

$$\Omega = \frac{\gamma+\delta\Omega'}{\alpha+\beta\Omega'}, \quad \omega = \frac{\gamma+\delta\omega}{\alpha+\beta\omega'} \tag{14}$$

Suppose first that all $\alpha, \beta, \gamma\ \delta \neq 0$. Consider the case $\alpha\beta > 0$. Since the signs of all numbers $\alpha, \beta, \gamma, \delta$ may be changed, we may assume $\alpha > 0$, $\beta > 0$. From $\alpha\delta-\beta\gamma = 1$ we have $\alpha\beta\gamma\delta > 0$, consequently $\gamma\delta > 0$ and since $\Omega > 0$ and $\Omega' > 0$ the first equality (14) shows that $\gamma > 0$, $\delta > 0$. If $\alpha+\beta\omega' < 0$, then $\alpha/\beta < -\omega' < 1$ and $\alpha < \beta$; if $\alpha+\beta\omega' > 0$, then the second equality (14) shows that $\gamma+\delta\omega' < 0$ from which $\gamma < \delta$. Inequality $\gamma < \delta$ combined with $\alpha\delta-\beta\gamma = 1$ shows again that $\alpha \leqq \beta$; in fact, for $\alpha > \beta$ we have $\alpha\delta \geqq (\beta+1)(\gamma+1)$ $= \beta\gamma+\beta+\gamma+1 > \beta\gamma+1$ which is impossible. Thus, in all the cases $0 < \alpha \leqq \beta$. Let us develop δ/β into a continued fraction with an even number of quotients: $\delta/\beta = [l_0, l_1, \ldots, l_{2n-1}]$ and assume $\delta'/\beta' = [l_0, l_1, \ldots, l_{2n-2}]$. Then from $\beta'\delta-\delta'\beta = 1$, $\alpha\delta-\beta\gamma = 1$ combined with inequalities $0 < \beta' \leqq \beta$, $0 < \alpha \leqq \beta$ we can conclude that $\beta' = \alpha$, $\delta' = \gamma$, i.e. $\Omega = [l_0, l_1, \ldots, l_{2n-1}, \Omega']$, $\omega = [l_0, l_1, \ldots, l_{2n-1}, \omega']$. Construct for form $f = (a, b, a_1)$ the period of reduced forms; let it be (9). Denoting, as before, the roots of form $f_{2n} = (a_{2n}, b_{2n}, a_{2n+1})$ by Ω_{2n}, ω_{2n} we obtain from (10), since a and a_{2n} are positive, that $\Omega = [|k|, |k_1|, \ldots, |k_{2n-1}|, \Omega_{2n}]$. Comparing this with $\Omega = [l_0, l_1, \ldots, l_{2n-1}, \Omega']$ we find, due to the uniqueness of the development of Ω into a continued fraction, that $|k| = l_0$, $|k_1| = l_1$, $\ldots$, $|k_{2n-1}| = l_{2n-1}$, $\Omega_{2n} = \Omega'$. From which, since $k < 0$, $k_1 > 0$, $k_2 < 0, \ldots$, we have $k = -l_0$, $k_1 = l_1, \ldots, k_{2n-1} = l_{2n-1}$ and then from (11) $\omega = [l_0, l_1, \ldots, l_{2n-1}, \omega_{2n}]$; Comparing this with $\omega = [l_0, l_1, \ldots, l_{2n-1}, \omega']$ we obtain $\omega_{2n} = \omega'$. Thus, the roots Ω_{2n}, ω_{2n} of the form f_{2n} coincide with the roots Ω', ω' of form f', and since the forms f_{2n}, f' have the same determinant, and their first coefficients are greater than zero, we have identically $f' = f_{2n}$, which proves the theorem for the case $\alpha\beta > 0$. For $\alpha\beta < 0$, we may take $\alpha > 0$, $\beta < 0$; from $\alpha\delta-\beta\gamma = 1$, we have $\gamma\delta < 0$. Since $\omega < 0$, the second equality (14) gives $\gamma+\delta\omega' < 0$; but γ and $\delta\omega'$ are of the same sign, consequently, $\gamma < 0$, $\delta > 0$. Noting that form f' transforms into f by the inverse transformation $\begin{pmatrix} \delta & -\beta \\ -\gamma & \alpha \end{pmatrix}$, all coefficients of which are positive, we conclude, from the case considered above, that

f is contained in the right hand side of the period of the form f', and, consequently, form f' is in the left part of the period of f. It remains to consider the case when among coefficients $\alpha, \beta, \gamma, \delta$ some may be zero. For $\alpha = 0$ we have $\gamma = \pm 1$ and the first coefficient of f' is equal to the third coefficient c of form f, which is impossible since it is assumed that $a' > 0$ in form $f' = (a', b', a_1')$. Similarly $\delta \neq 0$. For $\beta = 0$ we may assume $\alpha = \delta = 1$ and the second formula (14) gives $\omega = \gamma + \omega'$, from which, since $|\omega| < 1$, $|\omega'| < 1$, $\omega\omega' > 0$, we have $\gamma = 0$, i.e. $f = f'$. The same result is obtained for $\gamma = 0$. The theorem is proved.

§ 5. Periods of integral forms

Let us apply the above reasonings to integral forms. The conditions for a form $f(a, b, c)$ to be reduced i.e. $0 < \sqrt{d} - b < |a|$ and $|c| < \sqrt{d} + b$, $ac < 0$, of a given determinant $d > 0$, are satisfied only by a finite number of systems of integers a, b, c. Therefore, there is only a finite number of reduced forms having a given determinant d; moreover, it has been proved that every integral form of a given determinant d is equivalent to a reduced form (obviously, also integral) This shows that theorem 13 is true when $d > 0$ and is not a square. Let $f = (a, b, a_1)$ be a reduced form; we construct a period of reduced forms (9) corresponding to it. Since all the elements of this period are integral reduced forms of determinant d, and the number of such forms is finite, it follows that in the chain $f, f_1, f_2, \ldots$ at least one form is repeated. But each element of the chain determines completely its two neighbouring forms; consequently, the series $f_1, f_2, \ldots$ contains form f. Let $2n$ be the least (clearly, even) number for which $f_{2n} = f$; then $f_{2n+1} = f_1$, $f_{2n+2} = f_2, \ldots, f_{-1} = f_{2n-1}, \ldots$, i.e. the series $\ldots, f_{-1}, f, f_1, \ldots$ presents an infinite repetition of the same sequence of forms $f, f_1, \ldots, f_{2n-1}$. The remaining elements of the algorithm (9) also present a periodic repetition of $2n$ first elements, namely (in the notation of the previous section) $k_s = k_t$, $\Omega_s = \Omega_t$, $\omega_s = \omega_t$ for $s \equiv t \pmod{2n}$. It follows from the last theorem of the preceeding section that $f, f_1, \ldots, f_{2n-1}$ exhausts all reduced forms of determinant d, properly equivalent to form f. Therefore, all the reduced forms of determinant d split into a finite number of periods $f, f_1, \ldots, f_{2n-1}$; the number of these periods is equal to the number of distinct classes of forms.

Consider the equivalence of forms (§ 1) for the case of a positive non-square determinant d. If f, f' are two forms of the same determinant d, and we must find out whether they are equivalent or not, we transform them (§ 4) by means of substitutions S, S' into reduced forms f_0 and f_0' and find the period of form $f_0: f_0, f_1, \ldots, f_{2n-1}$. If f_0' is not contained among these forms, then f and f' are not equivalent (properly); if $f_0' = f_i$ and f_0 is transformed into f_i by substitution T, then f, f' are equivalent, namely f is transformed into f' by STS'^{-1}. The first problem of equivalence is thus solved. The second problem of equivalence (§ 2) was reduced to solution of the Pellian equation $t^2 - du^2 = \sigma^2$. First, a remark on number σ (this remark is applicable to every integer determinant $d \neq 0$). Number σ was defined as the greatest common divisor of numbers a, $2b$, c, if $f = (a, b, c)$ is a form of determinant d. It has been noted (§ 2) that either d/σ^2 is an integer, or $4d/\sigma^2$ is an integer of the form $4k+1$. Taking $d = \Delta s^2$, where Δ is square-free, it is easy to find all the values of σ. Firstly, σ may be equal to any divisor δ of s; in fact, the form $(\delta, 0, -d/\delta)$ has determinant d and the divisor of σ corresponding to it is δ. To these values of σ, for $\Delta \equiv 1 \pmod 4$ we must adjoin also the values $\sigma = 2\delta$ where δ runs through all divisors of s, for which s/δ is even; in fact, form $(2\delta, \delta, (\delta^2 - \Delta s^2)/2\delta)$ is an integral form of determinant d and for it $\sigma = 2\delta$. Moreover, since in the transformation of form f into an equivalent form the value of σ remains unchanged, we may find the reduced forms which have the above values of σ.

Let d be a positive non-square determinant, and let σ have one of its possible values. Take a reduced form $f = (a, b, a_1)$ of determinant d with possible values of σ, and let us construct its period $f_0, f_1, \ldots, f_{2n-1}$ (see (9)). Denoting, as in previous section, the absolute values of $k, k_1, k_2, \ldots$ by $l, l_1, l_2, \ldots$ and assuming $a > 0$ we have by (10) the following development of the first root of f: $\Omega = [l, l_1, l_2, \ldots, l_{2n-1}\Omega] = (P_{2n-1} + P_{2n}\Omega)/(Q_{2n-1} + Q_{2n}\Omega)$ (since $f_{2n} = f$), which show that f transforms into itself by substitution $\begin{pmatrix} Q_{2n-1} & Q_{2n} \\ P_{2n-1} & P_{2n} \end{pmatrix}$. The latter substitution enables us to use the formula (4) § 2:

$$Q_{2n-1} = \frac{T - bU}{\sigma}, \quad Q_{2n} = -\frac{a_1 U}{\sigma}, \quad P_{2n-1} = \frac{aU}{\sigma}, \quad P_{2n} = \frac{T + bU}{\sigma}$$

to determine the solution $T > 0$, $U > 0$ of equation $T^2 - dU^2 = \sigma^2$.

Let us prove that this is the least solution. In fact, if the opposite were true, there would exist a solution t, u, for which $0 < u < U$ and, consequently, $0 < t < T$; then the substitution (§ 2)

$$\begin{pmatrix} \frac{t-bu}{\sigma} & -\frac{a_1 u}{\sigma} \\ \frac{au}{\sigma} & \frac{t+bu}{\sigma} \end{pmatrix} = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$$

transforms f into itself. For the coefficients of this substitution we have $\alpha > 0$, $0 < \beta < Q_{2n}$, $0 < \gamma < P_{2n-1}$, $0 < \delta < P_{2n}$. By reasoning similar to that in the last theorem of the previous section, we find that δ/β is a convergent to a continued fraction $\Omega = [l, l_1, \ldots]$. Moreover, taking $\delta/\beta = [l, l_1, \ldots, l_{2n'-1}]$ we have $\Omega = [l, l_1, \ldots, l_{2n'-1}, \Omega]$ so that f coincides with $f_{2n'}$, i.e. with $(2n'+1)$th term of the series $f, f_1, f_2, \ldots$. But since $b < Q_{2n}$ we have $n' < n$ and thus f is contained among the forms $f_1, f_2, \ldots, f_{2n-1}$ which contradicts the assumption. The remaining solutions of $t^2 - du^2 = \sigma^2$ may be deduced entirely from the smallest solutions, T, U. First we note that for two solutions t, u; t', u' the relation $(t+u\sqrt{d})/\sigma \cdot (t'+u'\sqrt{d})/\sigma = (t''+u''\sqrt{d})/\sigma$ defines integers t'', u'' which are also a solution of the equation. Letting n in $((T+U\sqrt{d})/\sigma)^n = (t_n+u_n\sqrt{d})/\sigma$ take values $1, 2, 3, \ldots$, we obtain a series of solutions $t_n > 0$, $u_n > 0$, for which $u_1 < u_2 < u_3 < \ldots$. It is easy to show that these pairs t_n, u_n exhaust all solutions in positive integers. In fact, let a solution t, u satisfy $u_n < u < u_{n+1}$ then the numbers t', u' defined by

$$\frac{t'+u'\sqrt{d}}{\sigma} = \left(\frac{t+u\sqrt{d}}{\sigma}\right)\left(\frac{T-U\sqrt{d}}{\sigma}\right)^n$$

give a solution with $t' > 0$, $0 < u' < U$, which is impossible (L. Dirichlet [14], § 85). Thus, all solutions t, u of equation $t^2 - du^2 = \sigma^2$ are obtained from the least solution by the following formula (cf. § 12, ch. II)

$$\frac{t+u\sqrt{d}}{\sigma} = \pm\left(\frac{T+U\sqrt{d}}{\sigma}\right)^n, \qquad n = 0, \pm 1, \pm 2, \ldots \tag{15}$$

We can now find in its final form all representations of a given number $m \neq 0$ by a form $f = (a, b, c)$ of determinant $d > 0$ which appertain

to the same root of the congruence $n^2 \equiv d \pmod{m}$ (see (6) § 2). Taking

$$\frac{t_n+u_n\sqrt{d}}{\sigma} = \left(\frac{T+U\sqrt{d}}{\sigma}\right)^n, \qquad n = 0, 1, 2, 3, \ldots \tag{16}$$

we can say that if there exists one primitive representation $x_0 = d$, $y_0 = \gamma$ belonging to a given root, then all the remaining representations of this kind are obtained from

$$x = \frac{\varepsilon x_0}{\sigma} t_n - \eta \frac{bx_0+cy_0}{\sigma} u_n, \quad y = \frac{\varepsilon y_0}{\sigma} t_n + \eta \frac{ax_0+by_0}{\sigma} u_n, \tag{17}$$

$$\varepsilon = \pm 1, \quad \eta = \pm 1, \quad n = 1, 2, 3, \ldots$$

The improper representations of m by form f may also be split into sets, collecting into each set those representations x, y for which $(x, y) = \delta > 0$ has the same value u, and, in addition, x/δ, y/δ (i.e. the proper representation of number m/δ^2 by form f) belongs to the same root of the congruence $n^2 \equiv d \pmod{m/\sigma^2}$. Obviously, representations x, y belonging to the same set are expressed through one of them by means of the same formula (17).

In conclusion, let us pause on one property of solutions t_n, u_n (see (16)) of equation $t^2 - du^2 = \sigma^2$, which we shall need later. Let r be an arbitrary modulus, let us prove that k may be selected in such a way that for $i \equiv j \pmod{k}$ $(i > j \geqq 0)$, we always have $t_i \equiv t_j$, $u_i \equiv u_j \pmod{k}$ i.e. the residues of numbers (t_0, u_0), $(t_1, u_1), \ldots$ present a recurrent sequence of residues (t_0, u_0), $(t_1, u_1), \ldots$, (t_{k-1}, u_{k-1}) (Gauss [20], D. A. art., 201). Consider equation $t^2 - dr^2u^2 = \sigma^2$. It follows from the properties of σ that σ is a possible number also for determinant $d' = dr^2$, so that this equation has solutions. Denoting by T', U' the smallest solution of equation $t^2 - dr^2u^2 = \sigma^2$ we see that for some $n > 0$ we have $T' = t_n$, $U'r = u_n$. It is not hard to prove that $k = 2n$ satisfies our requirements. In fact, $u_k = (2t_n/\sigma)u_n \equiv 0 = u_0$, $t_k = (t_n^2 + du_n^2)\sigma = \sigma + (2d/\sigma)u_n^2 \equiv \sigma = t_0 \pmod{r}$. From identity

$$\frac{t_{k+1}+u_{k+1}\sqrt{d}}{\sigma} = \left(\frac{t_{n+1}+u_{n+1}\sqrt{d}}{\sigma}\right)\left(\frac{t_n-u_n\sqrt{d}}{\sigma} + \frac{2u_n\sqrt{d}}{\sigma}\right)$$

$$= \frac{T+u\sqrt{d}}{\sigma} + \frac{2u_n(u_{n+1}d+t_{n+1}\sqrt{d})}{\sigma^2}$$

we find $t_{k+1} = T+(2d/\sigma)u_n u_{n+1} \equiv t_1$, $u_{k+1} = U+(2t_{n+1}/\sigma)u_n \equiv u_1$ (mod r). After which the truth of congruences $t_{k+i} \equiv t_i$, $u_{k+i} \equiv u_i$ (mod r) for every number i follows from recurrence relations $t_{m+1} = (2T/\sigma)t_m - t_{m-1}$, $u_{m+1} = (2T/\sigma)u_m - u_{m-1}$ $(m = 1, 2, \ldots)$ deduced from identity $(t_{m+1}+u_{m+1}\sqrt{d})/\sigma = (t_m+u_m\sqrt{d})/\sigma \cdot (2T/\sigma - (T-U\sqrt{d})/\sigma)$.

§ 6. Forms, whose determinant is a square

It remains to consider the case when the determinant of an integral form $f = (a, b, c)$ is equal to a square h^2 where h is a positive integer. The reasonings of § 4 cannot be applied to such forms, since their roots are rational. Let us prove that form f is properly equivalent to just one form $(k, -h, 0)$ where k is an integer $\geqq 0$ and $< 2h$ (Gauss [20], D.A. art. 206-207). From $b^2-ac = h^2$ we have $c/(h-b) = -(h+b)/a$: assuming these fractions equal to β/δ, with $(\beta, \delta) = 1$ (which is possible since not all numbers a, c, $h-b$, $h+b$ are zeros), we define integers α, γ by the condition $\alpha\delta-\beta\gamma = 1$. Transforming f by substitution $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ we obtain a form (a', b', c') in which $b' = a\alpha\beta + b(\alpha\delta+\beta\gamma) + c\gamma\delta = -(h+b)\alpha\delta + b(\alpha\delta+\beta\gamma) + (h-b)\beta\gamma = -h$, $c' = a\beta^2 + 2b\beta\delta + c\delta^2 = -(h+b)\beta\delta + 2b\beta\delta + +(h-b)\beta\delta = 0$ i.e. $(a', b', c') = (a', -h, 0)$. Further, substitution $\begin{pmatrix} 1 & 0 \\ m & 1 \end{pmatrix}$ transforms this form into $(k, -h, 0)$ where $k = a'-2hm$, and clearly, with a suitable chosen m we have $0 \leqq k < 2h$.

Now, let two *reduced* forms $(k, -h, 0)$ and $(k', -h, 0)$ $(0 \leqq k < 2h, 0 \leqq k' < 2h)$ be properly equivalent, i.e. the first form transforms into the second by means of substitution $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$; then we have

$$\begin{aligned} k' &= k\alpha^2-2h\alpha\gamma, \quad -h = k\alpha\beta-h(\alpha\delta+\beta\gamma), \\ 0 &= k\beta^2-2h\beta\delta, \quad \alpha\delta-\beta\gamma = 1. \end{aligned} \tag{18}$$

The second and the third equalities give $\beta(k\alpha-2h\gamma) = 0$. If $\beta \neq 0$, then $k\alpha-2h\gamma = 0$, $k' = 0$, $k\beta-2h\delta = 0$; eliminating h in these equalities, we obtain $k(\alpha\delta-\beta\gamma) = k = 0$ and then (since $h \neq 0$) $\gamma = 0$, $\delta = 0$ which is impossible. Consequently, $\beta = 0$, $\alpha = \delta = \pm 1$,

and the first equality (18) gives $k' = k - 2h\alpha\gamma \equiv k \pmod{2h}$ from which $k' = k$, $\gamma = 0$. Therefore, the forms $(k, -h, 0)$ and $(k', -h, 0)$ are properly equivalent only when they coincide and the transforming substitution is $\begin{pmatrix} \pm 1 & 0 \\ 0 & \pm 1 \end{pmatrix}$. The statement is proved. From the above reasoning it is clear also that the reduced form $(k, -h, 0)$ (and, consequently every form of determinant h^2) is transformed into itself only by means of two substitutions $\begin{pmatrix} \pm 1 & 0 \\ 0 & \pm 1 \end{pmatrix}$ of determinant 1, and by no other substitution (which also follows from general reasonings of § 2). The above reduction of forms allows us to see, as before, whether the forms f and f' of determinant h^2 are properly equivalent; and, if they are, to find the transformation of one into another; and this is the only transformation of f into f', apart from possible change of sign. Solution of the problems on equivalence of forms leads to the determination of all representations of a given number $m \neq 0$ by a given form (see §§ 1–2), of determinant h^2, of which there is, obviously, a finite number. In conclusion, let us note that the theorem proved above on the reduction of forms of determinant h^2 may be formulated as follows: *a given form* (a, b, c) *of determinant* h^2 *determines completely a number* $k \geqq 0$, $k < 2h$ *and four numbers* α, λ, γ, δ, $(\alpha\delta - \beta\gamma = 1)$ *for which* $(k, -h, 0) \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = (a, b, c)$ (*apart from possible change of sign in all* α, β, γ, δ). We shall need this theorem later (§ 4, ch. VI).

§ 7. Solution of a general quadratic equation in two unknowns

In the previous sections we obtained all that is necessary for the solution in integers z, t of a general equation of second degree

$$az^2 + 2bzt + ct^2 + 2mz + 2nt + p = 0 \tag{19}$$

with integer coefficients a, b, c, m, n, p (Gauss [20], D.A. art. 216). First, consider the case $b^2 - ac \neq 0$. Denoting by $-f$, $-e$, $-d$ the cofactors of the second row of determinant

$$\Delta = \begin{vmatrix} a & b & m \\ b & c & n \\ m & n & p \end{vmatrix},$$

we introduce, instead of z, t the integers $x = dz-f, y = dt-e$. Then equation (19) becomes

$$ax^2+2bxy+cy^2 = (b^2-ac)\Delta = d\Delta \tag{20}$$

The problem reduces to finding of all solutions of the equation in integers x, y and choosing those for which

$$z = \frac{x+f}{d}, \quad t = \frac{y+e}{d} \tag{21}$$

are integers. These integers are, in fact, the solutions of equation (19). If $b^2-ac = d < 0$, then equation (20) has a finite number of solutions. We find them by the rules of §§ 1–3, and then obtain by (21) all solutions of (19) of which there also is a finite number (which is also obvious geometrically, since equation (19) represents an ellipse in the plane zt). If $b^2-ac > 0$ and is not a square, then for $\Delta = 0$ equation (20) has only one solution $x = 0$, $y = 0$. For $\Delta \neq 0$,we have seen in § 5 that all the solutions of equation (20) are contained in a finite number of formulae of the form $x = At_n/\sigma+Bu_n/\sigma$, $y = Ct_n/\sigma+Du_n/\sigma$ $(n = 1, 2, 3, \ldots)$ where A, B, C, D are integers, σ is the greatest common divisor of a, $2b$, c and t_n, u_n are positive solutions of the Pellian equation $t^2-du^2 = \sigma^2$ determined from the smallest solution T, U by formula (16) (see formulae (17)). Substituting these values of x, y into (21) we find

$$z = \frac{At_n+Bu_n+\sigma f}{\sigma d}, \quad t = \frac{Ct_n+Du_n+\sigma e}{\sigma d}, \qquad n = 1, 2, 3, \ldots \tag{22}$$

To select all n for which these numbers are integers, we use the concluding statement of § 5. Let us find for modulus $r = \sigma d$ a number k such that $t_i \equiv t_j$, $u_i \equiv u_j \pmod{r}$ if $i \equiv j \pmod{k}$. Let n', n'', ... be the values of n, $n > 0$, and $n < k$, for which the right hand sides of the formula (22) are integers. Clearly, all the remaining values of this type are congruent to n', n'', ... modulo k. Thus, for a given set of solutions x, y of equations (20) we can select, by means of a finite number of operations, all the corresponding solutions z, t of equation (19). The same can be done with all other sets of solutions of (20), after which we find all solutions of (19). Finally, if $b^2-ac > 0$ and is a square, then for $\Delta \neq 0$ equation (20), and, consequently, (19) has a finite number of solutions, which are all of the form

$x = \alpha u$, $y = \beta u$ where α, β are given and $u = 0, \pm 1, \pm 2, \ldots$ are arbitrary integers. Substituting this in (21) we obtain $z = (\alpha u+f)/d$, $t = (\beta u+e)/d$ and the selection of integer values of z, t is reduced to solving a linear congruence. Now, consider the case when in the given equation (19) we have $b^2-ac = 0$ (but not all a, b, c are zero). It is easy to see that in this case $az^2+2bzt+ct^2 = \delta(\alpha z+\beta t)^2$ where δ, α, β are integers. Put $\alpha z+\beta t = u$, for integral z, t these are integers. Determining z, t from equations $\delta u^2+2(mz+nt)+p = 0$, $\alpha z+\beta t = u$ we find for $\alpha n-\beta m \neq 0$

$$z = \frac{\beta\delta u^2+2nu-\beta p}{2(\alpha n-\beta m)}, \quad t = \frac{-\alpha\delta u^2-2mu+\alpha p}{2(\alpha n-\beta m)},$$

The problem is reduced to selecting all integers $u = 0, \pm 1, \pm 2, \ldots$ for which the above expressions are integers. This requires solving a quadratic congruence. Finally, for $\alpha n-\beta m = 0$ equation (19) is of the form $\delta u^2+2\varepsilon u+p = 0$ (ε is independent of z, t). For solubility of (19) this quadratic equation must have at least one integer root, after which z and t are found by solving an indeterminate linear equation. Thus, the above method enables us to solve equation (19) completely for all cases.

§ 8. Order of forms. Representation of numbers by a complete system of non-equivalent forms of a given order

From now on we shall be concerned exclusively with integral forms whose determinant is not a perfect square (and, consequently, not equal to zero). Let $\sigma > 0$ be the greatest common divisor of a, $2b$, c for the form (a, b, c) of determinant d. The set of all forms having the same d, σ (for $d < 0$) with the same sign of the end coefficients a, c is called the *order* of forms (ordo by Gauss [20] D.A. art. 226). Since d, σ and the signs of a, c remain unchanged when a form is transformed into an equivalent one, the order is a set of several classes. When $\sigma = 1$, the forms and the order are called *properly primitive* (formae proprie primitivae, according to Gauss, or eigentlich primitive in present German terminology). For $\sigma = 2$ and $d \equiv 1 \pmod 4$ the forms are called *improperly primitive* (Improprie primitivae, uneigentlich primitive). It was noted earlier in § 2 that either d/σ^2 is an integer, or $4d/\sigma^2$ is an integer of the form $4n+1$; in the first

case, the form $(a/\sigma, b/\sigma, c/\sigma)$ is properly primitive, in the second case the form $(2a/\sigma, 2b/\sigma, 2c/\sigma)$ is improperly primitive. The form $(\sigma, 0, -d/\sigma)$ for $d \equiv 0 \pmod{\sigma^2}$ and the form $(\sigma, \frac{1}{2}\sigma, (\sigma^2 - 4d/4\sigma))$ for $4d \equiv \sigma^2 \pmod{4\sigma^2}$ are called the *simplest* forms (forma simplissima). Finally, the form $(1, 0, -d)$ is called the *principal* form (forma principalis) and its class – the *principal* class of determinant d. Consider an arbitrary a properly primitive or an improperly primitive order of determinant d, positive for $d < 0$ and let us select one form out of every class. These forms $f_i(a_i, b_i, c_i)$ $(i = 1, 2, \ldots, h)$ present a complete system of non-equivalent forms of a given order. For $d < 0$ all a_i are, by assumption, greater than zero; for $d > 0$ we may also assume $a_i > 0$ replacing, if necessary the form f_i by a form equivalent to it. Let $m > 0$ be an integer, for which $(m, 4d) = \sigma$ where $\sigma = 1$ for a properly and $\sigma = 2$ for an improperly primitive order. For the existence of proper representations of m by a *system* of forms, it is necessary that d is a quadratic residue of m (§ 1); assuming this condition satisfied, take a root of congruence $n^2 \equiv d \pmod{m}$. Assuming $(n^2 - d)/m = l$ we see from condition $(m, 4d) = \sigma$ that the greatest common divisor of $m, 2n, l$ is equal to σ; consequently, the form (m, n, l) belongs to the same order, and thus it is equivalent to one of the forms f_i. If $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ runs through all substitutions transforming f_i into (m, n, l), then the numbers α, γ give all the proper representations of m by a form f_i, which belong to the root n (§ 1). The number of such representations for $d < 0$ is, in general, equal to 2; for $d = -1$ it is equal to 4; and for $d = -3$, $\sigma = 2$, it is equal to 6 (§ 2); for $d > 0$ the number of proper representations of m by form f_i, which belongs to the same root of congruence $n^2 \equiv d \pmod{m}$ is infinite and they are all obtained from the same α, γ by means of formulae (6), (§ 2), in which a, b, c are replaced by a_i, b_i, c_i of form f_i and t, u denote all solutions of equation $t^2 - du^2 = \sigma^2$. In order to select from these representations one particular one, let us note that

$$\begin{aligned} a_i m &= a_i(a_i\alpha'^2 + 2b_i\alpha'\gamma' + c_i\gamma'^2) \\ &= (a_i\alpha' + b_i\gamma' + \gamma'\sqrt{d})(a_i\alpha' + b_i\gamma' - \gamma'\sqrt{d}) \end{aligned} \tag{23}$$

and, by using (6), § 2 and (15) § 5, (T, U is the least solution of equation $t^2 - du^2 = \sigma^2$), we have

$$a_i\alpha'+b_i\gamma'+\gamma'\sqrt{d} = (a_i\alpha+b_i\gamma+\gamma\sqrt{d})\frac{t+u\sqrt{d}}{\sigma}$$

$$= \pm(a_i\alpha+b_i\gamma+\gamma\sqrt{d})\left(\frac{T+U\sqrt{d}}{\sigma}\right)^k, \qquad k = 0, \pm1, \pm2, \ldots$$

The sign $\pm$ and the index k are uniquely determined from

$$\sqrt{a_i m} \leqq a_i\alpha'+b_i\gamma'+\gamma'\sqrt{d} < \sqrt{a_i m}\,\frac{T+U\sqrt{d}}{\sigma} \tag{24}$$

from which, by (23), we have

$$a_i\alpha'+b_i\gamma'-\gamma'\sqrt{d} \leqq a_i\alpha'+b_i\gamma'+\gamma'\sqrt{d},$$

$$(a_i\alpha'+b_i\gamma'+\gamma'\sqrt{d})\frac{T-U\sqrt{d}}{\sigma} < (a_i\alpha'+b_i\gamma'-\gamma'\sqrt{d})\frac{T+U\sqrt{d}}{\sigma}$$

i.e. $\gamma' \geqq 0$, $U(a_i\alpha'+b_i\gamma') > T\gamma'$. Conversely, from these inequalities follow inequalities (24). Thus, taking $\varkappa = 4$ for $d = -1$, $\varkappa = 6$ for $d = -3$, $\sigma = 2$; $\varkappa = 2$ for the remaining $d < 0$; and $\varkappa = 1$ for $d > 0$, we may say that the number m, for which d is a quadratic residue, has $\varkappa 2^{(m)}$ proper representations by a system of forms f_i, where (m) is the number of distinct odd prime divisors of m, and where for $d > 0$ the numbers α, γ are subject to the above linear inequalities. Let an integer $m > 0$ be given by the only condition $(m, 4d) = \sigma$. Collecting into one set all the representations of m by a system of forms f_i in which the representation numbers have the same greatest common divisor $\delta > 0$ (clearly, odd) we find that the number of all representations of m by a system of forms f_i is expressed as follows: $\varkappa \sum 2^{(m')}$, where the summation is performed over all square divisors δ of m, for which d is a quadratic residue of $m' = m/\delta^2$. By a similar reasoning to ch. II (§ 81)) we obtain $\varkappa \sum 2^{(m')} = \varkappa \sum (d/\sigma)$ where the summation is preformed over all odd divisors δ of m. Thus, we obtain the following theorem: *Given a complete system of non-equivalent forms $f_i = (a_i, b_i, c_i)$ of properly or improperly primitive order of determinant d, with positive first coefficients c_i; and a number $m > 0$ for which $(m, 4d) = 1$ for properly and $= 2$ for improperly primitive order. The number of representations of m by a system of*

forms f_i is equal to $\varkappa\sum(d/\sigma)$ where the summation is performed over the odd divisors δ of m and $\varkappa$ is as defined above. Moreover, for $d > 0$ to every equation $m = a_i x^2 + 2b_i xy + c_i y^2$ are added auxiliary conditions $y \geqq 0$, $U(a_i x + b_i y) > Ty$. Analytical interpretation of the fact expressed in the theorem has led Dirichlet (L. Dirichlet [14], V. Abschn.) to the discovery of his famous formulae for the number of classes of binary forms (see § 3, ch. IV). In particular cases 1) $d = -1$, 2) $d = -2$, 3) $d = -3$, $\sigma = 1$, 4) $d = -3$, $\sigma = 2$, 5) $d = 2$ the system of forms f_i contains only one form, which may be taken to be 1) $x^2 + y^2$, 2) $x^2 + 2y^2$, 3) $x^2 + 3y^2$, 4) $2x^2 + 2xy + 2y^2$, 5) $x^2 - 2y^2$, and again we obtain theorems which have been proved before by a different method (§ 8, ch. II, 1–4, and § 4, ch. III). It should be mentioned that inequalities $x \pm 2y > 0$ given for the form $x^2 - 2y^2$ in § 8, ch. II, do not coincide with inequalities $2x > 3y \geqq 0$ of the theorem of the present section. But the connection between the two may easily be established.

§ 9. Ambiguous forms and classes. A special study of the periods of indefinite forms

Two forms (a, b, c) and $(a, -b, c)$ as well as their classes are said to be *opposite* forms and classes. If K denotes one of these classes, then the other is denoted by K^{-1}. Since (a, b, c) is transformed into $(a, -b, c)$ by substitution $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ of determinant -1, it follows from the multiplication rules for substitutions (§ 3, ch. II) that every form of class K is improperly equivalent to every form from K^{-1} and, conversely, in case of improper equivalence of two forms their classes are opposite. The class which is its own opposite is said to be an *ambiguous* class (ambige Klasse by Kummer, zweiseitige by Dedekind), every form of such class is improperly equivalent to itself. The form (a, b, c) in which $2b$ is divisible by a (the determinant of this form, by supposition of § 8 is not a square, and consequently $a \neq 0$), is called an *ambiguous* form. This form is transformed into itself by substitution $\begin{pmatrix} 1 & 2b/a \\ 0 & -1 \end{pmatrix}$, and, consequently, it belongs to an ambiguous class. To prove the converse statement: *every ambiguous class contains*

at least one ambiguous form; let $f = (a, b, c)$ be a form of a given ambiguous class, and let $fS = f'$ where $S = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ is an integral substitution of determinant -1. From $a\alpha\beta + b(\alpha\delta + \beta\gamma) + c\gamma\delta = b$ and $\beta\gamma = \alpha\delta + 1$ we find $a\alpha\beta + (2b\alpha + c\gamma)\delta = 0$ which together with $a\alpha^2 + (2b\alpha + e\gamma)\gamma = a$ gives $-a\alpha = a\delta$ i.e. $\delta = -\alpha$. If $\gamma = 0$, then $\delta = -\alpha = \pm 1$ and clearly the form f is itself ambiguous. Taking $\gamma \neq 0$, take a substitution $T = \begin{pmatrix} \xi & \eta \\ \zeta & \theta \end{pmatrix}$ of determinant 1, which transforms f into φ; then φ transforms into itself by substitution $T^{-1}ST = \begin{pmatrix} \alpha' & \beta' \\ \gamma' & -\alpha' \end{pmatrix}$ of determinant -1 and if we choose T in such a way that $\gamma' = 0$, then the form φ is, by the above, an ambiguous form. Equality $\gamma' = \gamma\xi^2 - 2\alpha\xi\zeta - \beta\zeta^2 = 0$ is equivalent to: $(\gamma\xi - \alpha\zeta)^2 = \zeta^2$. This condition is satisfied if we assume ξ and ζ to be the numerator and the denominator of an irreducible fraction equal to $(\alpha + 1)/\gamma$ then we choose η and θ to satisfy the condition $\xi\theta - \eta\zeta = 1$, and obtain the substitution T transforming f into an ambiguous form equivalent to it. The proved theorem presents a particular case of the following theorem of Gauss (D.A. [20], art. 164): if the form f contains form f' either properly or improperly, then there exists an ambiguous form contained in f and containing f'.

In the case of a positive determinant every class of forms is characterised by its period of reduced forms (§ 4). In order to establish the connection between the periods of opposite classes, we shall call the forms $f = (a, b, c)$ and $\bar{f} = (c, b, a)$ the *associated* forms. Clearly, these forms belong to opposite classes. A form $\bar{f}$ is reduced simultaneously with f (§ 4); also, if f is transformed by substitution $\begin{pmatrix} 0 & -1 \\ 1 & k \end{pmatrix}$ into its right neighbouring form f_1 (§ 3, ch. II), then the same substitution transforms $\bar{f}_1$ into $\bar{f}$. Therefore, it f is a reduced form, and if $f, f_1, f_2, \ldots, f_{2n-1} f_{2n} = f$ is its period, then $\bar{f}_{2n} = \bar{f}, \bar{f}_{2n-1}, \ldots, \bar{f}$, is the period of the associated form. Thus, the period of the opposite class is obtained by passing on to the associated forms and writing them in the reverse order (*associated periods*). We do not give a detailed exposition on these concepts here since they coincide, in their essence, with the concepts described in § 11, ch. II (Galois theorem). If f is a reduced form of an *ambiguous* class, then $\bar{f}$, as a

reduced form equivalent to f, is contained in the period of the form f (§ 4); again, denoting this period of f by $f, f_1, \ldots, f_{2n-1}$ and noting that the first coefficients of f and $\bar{f}$ have opposite signs, we may take $\bar{f} = f_{2i+1}$. But, since a reduced form has only one right (and only one left) reduced neighbouring form (§ 4), it follows that $\bar{f}_1 = f_{2i}$, $\bar{f}_2 = f_{2i-1}, \ldots, \bar{f}_i = f_{i+1}$; consequently, for $f_{i+1} = (a, b, c)$ its left neighbouring form is (c, b, a) from which, by the definition of the neighbouring forms (§ 3, ch. II) it follows that $2b \equiv 0 \pmod{a}$, i.e. f_{i+1} is an ambiguous form. From the same relation $\bar{f} = f_{2i+1}$ we have $\bar{f}_{2i+1} = f_{2n}$, $\bar{f}_{2i+2} = f_{2n-1}, \ldots, \bar{f}_{n+i} = f_{n+i+1}$ i.e. f_{n+i+1} is also an ambiguous form; Forms f_{i+1} and f_{n+i+1} are distinct since their indices are incongruent modulo $2n$. If the period of f contains another ambiguous form f_{k+1} the forms f_k, f_{k+1} are associated and so are the forms f_{k-1}, f_{k+2}, etc. and finally forms f, f_{2k+1}; from $\bar{f} = f_{2k+1}$, $\bar{f} = f_{2i+1}$ we find $f_{2k+1} = f_{2i+1}$, $2k \equiv 2i \pmod{2n}$, $k \equiv i$ or $i+n \pmod{2n}$ i.e. form f_{k+1} coincides with f_{i+1} or f_{n+i+1}. Thus, in every ambiguous class of a positive determinant there exist two and only two *reduced* ambiguous forms (Gauss, D.A. [20] art. 187).

We have seen that the periods of opposite classes are in a certain relationship with one another (i.e. they are associated). It is important to note another symmetry which exists for periods (and classes) of a positive determinant. Namely, to every reduced form $f = (a, b, c)$ there corresponds a reduced form $f' = (-a, b, -c)$ whose roots (§ 4) differ from the corresponding roots of f by a sign only. It is easy to see that if $f\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = f_1$, then $f'\begin{pmatrix} -\alpha & \beta \\ \gamma & -\delta \end{pmatrix} = f_1'$; therefore, if $f, f_1, \ldots, f_{2n-1}$ is the period of the form f, then $f', f_1', \ldots, f_{2n-1}'$ is the period of form f' moreover, the substitution $\begin{pmatrix} 0 & -1 \\ 1 & k_i \end{pmatrix}$ transforming f_i into f_{i+1} in the first period, corresponds to the substitution $\begin{pmatrix} 0 & -1 \\ 1 & -k_i \end{pmatrix}$ in the second. Thus, to every class of determinant $d > 0$ (class of form f), there corresponds a symmetric to it class (class of form f'). To find when two symmetric classes coincide, we must solve the question of equivalence of forms f and f'; considering this question similarly to that of the transformation of form into itself, we find that all substitutions transforming $f = (a, b, c)$ into f' are of the form

$$\begin{pmatrix} \frac{t-bu}{\sigma} & \frac{cu}{\sigma} \\ \frac{au}{\sigma} & -\frac{t+bu}{\sigma} \end{pmatrix},$$

where σ is the greatest common divisor of a, $2b$, c and t, u run through all integral solutions of equation $t^2-du^2 = -\sigma^2$. Consequently, for two symmetric classes to coincide, it is necessary that equation $t^2-du^2 = -\sigma^2$ has solutions, in which case every class of the order defined by d, σ coincides with its symmetric class. The condition of coincidence of symmetric classes may be given in another form (Dirichlet [14], § 83). If f is a reduced form, and f' is equivalent to f, then f' occurs in the period of f, i.e. in $f, f_1, \ldots, f_{2n-1}$. Let $f' = f_i$; then $f_1' = f_{i+1}, f_2' = f_{i+2}, \ldots, f_i' = f_{2i}$ i.e. $2i \equiv 0 \pmod{2n}$, from which $i = n$ and n is odd (since the first coefficients in f and $f_i = f'$ are of the opposite sign). Assuming the notations of § 4 (formulae (9) and (12)), we may say that $f_{\nu+n} = f_\nu'$, $k_{\nu+n} = -k_\nu$, $l_{\nu+n} = l_\nu$ for every ν, and that the first root of f develops into the continued fraction $|\Omega| = [l, l_1, \ldots]$ whose period $l, l_1, \ldots, l_{n-1}$ is half the length of the period of form f. Conversely, it is easy to show that if the period of the continued fraction of $|\Omega|$ is shorter than the period of the form f, then the symmetric classes coincide. Let us apply these results to the case when $d = p$ is a prime of the form $4n+1$. In this case equation $x^2-py^2 = -1$ has solutions (§ 12, ch. II), and in the properly primitive order the symmetric classes coincide. Let $f = (1, \lambda, \lambda^2-p)$ (where $\lambda = [\sqrt{p}]$) be a reduced form of the principal class, and let $f, f_1, \ldots, f_{2n-1}$ be its period. As was just mentioned, n is odd and $f_{n+i} = f_i'$ for every i. On the other hand, f is an ambiguous form and therefore f_i and f_{2n-i-1} are associate for every i (see above). Therefore, taking $f_{\frac{1}{2}(n-1)} = (a, b, -a')$ we obtain $f_{\frac{1}{2}(2n-1)} = (-a', b, a) = (-a, b, a')$ i.e. $a' = a, p = b^2+aa' = b^2+a^2$. Thus, we obtain a method of expressing a prime p as a sum of two squares by evaluating the period of the forms of determinant p, or, (which is the same) from the development of $\sqrt{p}$ into a continued fraction. (Gauss [20], D.A. art. 265). Similar results on the representation of primes by forms $b^2 \pm 2a^2$ are given in the dissertation of Göeppel (see Përron [69], p. 109). Below, we shall find useful the solution of the following question: how many different ambiguous classes are there in the

properly primitive order of determinant d? By the above proof, every ambiguous class has an ambiguous form, therefore, for our purpose it suffices to find out how many non-equivalent properly primitive forms of determinant d are there, which are positive for $d < 0$. First, we note that a given form (a, b, c) may be transformed by $\begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix}$ into a form (a, b', c') in which the middle coefficient $b' = b + ak$ is any number congruent to b modulo a. (Such forms are called *parallel*). Let $f = (a, b, c)$ be an ambiguous form. Since $2b \equiv 0 \pmod{a}$ we have either $b \equiv 0$ or $b \equiv \frac{1}{2}a \pmod{a}$. In the first case f is parallel to form $f_0 = (a, 0, a')$, where $-d = aa'$, in the second case it is parallel to form $f_1 = (a, \frac{1}{2}a, (a^2 - 4d)/4a) = (2b, b, \frac{1}{2}(b + b'))$ where $b = \frac{1}{2}a$ and b' are integers satisfying $-d = bb'$. Denote by (d) the number of distinct odd divisors of d; since $f_0 = (a, 0, a')$ is a properly primitive form, we have $(a, a') = 1$ and consequently, the number of forms f_0 (with $a \gtrless 0$) is $2^{(d)+1}$ when d is odd, and $2^{(d)+2}$ when d is even. In the form $f_1 = (2b, b, \frac{1}{2}(b + b'))$ the numbers b, b' have no common divisor, and satisfy the congruence $b + b' \equiv 2 \pmod{4}$; from this it is easy to deduce that for an odd d the forms f_1 exist only if $d \equiv -1 \pmod{4}$ in which case their number is $2^{(d)+1}$. For an even d they exist only if $d \equiv 0 \pmod{8}$ and their number is $2^{(d)+2}$. The total number of forms f_0, f, equals, consequently to $2^{(d)+1}$ for $d \equiv 1 \pmod{4}$, $2^{(d)+2}$ for $d \equiv -1, 2 \pmod{4}$, and for $d \equiv 4 \pmod{8}$; $2^{(d)+3}$ for $d \equiv 0 \pmod{8}$. We shall prove that the required number of ambiguous classes is always four times less. This is true for $d = -1$, since then there exists only one class $(1, 0, 1)$. Taking $|d| > 1$ we may say that in the factorisations $-d = aa'$ (for forms f_0) and $-d = bb'$ (for forms f_1) the absolute values of the factors a, a' (or b, b') are distinct; but since $(a, 0, a')\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = (a', 0, a)$, and $(2b, b, \frac{1}{2}(b + b'))$ $\begin{pmatrix} -1 & -1 \\ 2 & 1 \end{pmatrix} = (2b', b', \frac{1}{2}(b' + b))$, we may assume that $|a| < |a'|$ in forms f_0 and $|b| < |b'|$ in forms f_1, which diminishes the number of these forms by half. First, let $d < 0$; assuming the outside coefficients in f_0, f_1 to be positive (which diminishes the number of such forms by half again) we have $0 < a < a'$ for $f_0 = (a, 0, a')$ so that f_0 is a reduced form (see inequalities (8) § 3). Each form $f_1 = (2b, b, \frac{1}{2}(b + b'))$ in which $0 < 3b < b'$ is also a reduced form; if $b < b' < 3b$ then we

replace f_1 by its right neighbouring form $(\frac{1}{2}(b+b'), \frac{1}{2}(b'-b), \frac{1}{2}(b+b'))$. which is reduced. All reduced forms thus obtained are, clearly, distinct, and therefore they belong to distinct classes (§ 3); and these are the required ambiguous classes, since it is clear from the above that every positive properly primitive ambiguous form of determinant d is equivalent to one of these forms. Next let $d > 0$. All forms f_0, f_1 with the above restrictions $|a| < |a'|$ and $|b| < |b'|$ are distinct. Denoting each of them by (A, B, C) we replace it by a parallel form (A, B', C') in which B' is defined by conditions $B' \equiv B \pmod{A}$, $\sqrt{d}-|A| < B' < \sqrt{d}$. All forms (A, B', C') are distinct; moreover, they are all reduced (§ 4). In fact, for $|A| < \sqrt{d}$ we deduce from inequalities for B': $\sqrt{d}-B' < |A| < \sqrt{d}+B'$, $B' < \sqrt{d}$. This by § 4 means that (A, B', C') is reduced. The case $|A| > \sqrt{d}$ may occur only when the form (A, B, C) coincides with one of the forms $f_1 = (2b, b, \frac{1}{2}(b+b'))$ and since in this form $|b| < \sqrt{d}$ we have $A = 2B$, $B' = |B|$ and, again, we have $0 < \sqrt{d}-B' < |A| < \sqrt{d}+B'$. Finally, let us prove that every reduced properly primitive ambiguous form (a, b, c) coincides with one of the forms (A, B', C'). If $b \equiv 0 \pmod{a}$ then from $0 < b < \sqrt{d}$ we have $|a| < \sqrt{d}$; the form (a, b, c) is parallel to the form $(a, 0, a')$, and since in this form $aa' = -d$, $|a| < \sqrt{d}$, it coincides with one of the forms $f_0 = (A, B, C)$, and then the corresponding form (A, B', C') coincides with (a, b, c) so that b, as the middle coefficient of a reduced form, satisfies the same conditions as B'. If b is not divisible by a, then, from $2b \equiv 0 \pmod{a}$, we have $|a| < 2\sqrt{d}$; then similarly to the above, we find that (a, b, c) is parallel to one of the forms f_1 and coincides with the corresponding form (A, B', C'). Thus, the forms (A, B', C') exhaust all reduced ambiguous forms. However, it has been proved above that every ambiguous class of positive determinant contains two and only two reduced ambiguous forms. Consequently, the number of ambiguous classes is half the number of forms (A, B', C') i.e. half of the number of the forms f_0, f_1. Thus, we obtain the following theorem: *the number of properly primitive ambiguous classes of determinant d (positive for* $d < 0$*) is equal to* $2^{(d)-1}$ *for* $d \equiv 1 \pmod 4$; $2^{(d)}$ *for* $d \equiv 2, 3 \pmod 4$ *or* $d \equiv 4 \pmod 8$ *and to* $2^{(d)+1}$ *for* $d \equiv 0 \pmod 8$. (Gauss [20] D. A. art. 257–258, L. Dirichlet [14], 153).

§ 10. The composition of binary forms

Gauss's *theory of composition* (D. A. [20], art. 234–244) reveals the connection between different classes of forms. If the forms

$$\begin{aligned} F(X, Y) &= AX^2+2BXY+CY^2, \quad f(x, y) = ax^2+2bxy+cy^2 \\ f'(x', y') &= a'x'^2+2b'x'y'+c'y'^2 \end{aligned} \tag{25}$$

are such, that on replacing X, Y by bilinear expressions

$$\begin{aligned} X &= pxx'+p'xy'+p''yx'+p'''yy' \\ Y &= qxx'+q'xy'+q''yx'+q'''yy' \end{aligned} \tag{26}$$

we obtain, identically in X, y, x', y'

$$F(X, Y) = f(x, y)f'(x', y'),$$

then it is said that the form F is *transformable into a product of forms* f, f' (transformabilis in productum). Coefficients $p, p', \ldots, q'''$ of the transformation (26) are assumed to be integers. If, in addition, the determinants

$$\begin{aligned} P &= \begin{vmatrix} p & p' \\ q & q' \end{vmatrix}, \quad Q = \begin{vmatrix} p & p'' \\ q & q'' \end{vmatrix}, \quad R = \begin{vmatrix} p & p''' \\ q & q''' \end{vmatrix}, \\ S &= \begin{vmatrix} p' & p'' \\ q' & q'' \end{vmatrix}, \quad T = \begin{vmatrix} p' & p''' \\ q' & q''' \end{vmatrix}, \quad U = \begin{vmatrix} p'' & p''' \\ q'' & q''' \end{vmatrix} \end{aligned} \tag{27}$$

are integers without a common factor, then form F is said to be *composed or compounded* (composita) from forms f, f'. Equating in $F = ff'$ the coefficients of $x^2x'^2$, $x^2x'y', \ldots$ we find that this equality is equivalent to the following nine relations between the coefficients of forms (25) and the transformation (26):

$$\begin{aligned} &Ap^2+2Bpq+Cq^2 = aa' \\ &Ap'^2+2Bp'q'+Cq'^2 = ac' \\ &Ap''^2+2Bp''q''+Cq''^2 = ca' \\ &Ap'''^2+2Bp'''q'''+Cq'''^2 = cc' \\ &App'+B(pq'+p'q)+Cqq' = ab' \\ &App''+B(pq''+p''q)+Cqq'' = ba' \\ &Ap'p'''+B(p'q'''+p'''q')+Cq'q''' = bc' \\ &Ap''p'''+B(p''q'''+p'''q'')+Cq''q''' = cb' \\ &A(pp'''+p'p'')+B(pq'''+p'''q+p'q''+p''q)+C(qq'''+q'q'')=2bb' \end{aligned} \tag{28}$$

From these relations Gauss successively draws the following conclusions (D. A. [20], art. 235): 1) if D is the determinant of the form F, which is transformable into the product of forms f, f' of determinants d, d', then $d = Dn^2$, $d' = Dn'^2$ where n, n' are rational numbers, which are defined, together with their signs, below. 2) Between determinants (27) and the coefficients of forms f, f' the following relations hold: $P = an'$, $R-S = 2bn'$, $U = cn'$, $Q = a'n$, $R+S = 2b'n$, $T = c'n$. 3) If $m > 0$ is the *divisor* of form f (i.e. the greatest common divisor of $a, 2b, c$); if m' is the divisor of f' and k is the greatest common divisor of determinants (27), then Dk^2 is the greatest common divisor of dm'^2 and $d'm^2$. In particular, if F is compounded of f and f' ($k = 1$), then its determinant is the greatest common divisor of dm'^2 and $d'm^2$, i.e. it is completely determined by forms f and f'; 4) the divisor of form F which is compounded of f and f' is equal to the product mm' of divisors of these forms; 5) if F is transformable into ff', then

$$\begin{gathered} an' = P, \quad 2bn' = R-S, \quad cn' = U, \\ a'n = Q, \quad 2b'n = R+S, \quad c'n = T, \\ Ann' = q'q''-qq''', \quad 2Bnn' = pq'''+p'''q-p'q''-p''q', \\ Cnn' = p'p''-pp'''. \end{gathered} \tag{29}$$

Conversely, if between the coefficients of the forms (25) and the coefficients of the substitution (26) there exist nine relations (29) with some rational n, n', not equal to zero, then all relations (28) hold (i.e. F is transformed into ff' by substitution (26)) and $n = \sqrt{d}/D$, $n' = \sqrt{d'}/D$. It is easy to deduce from the definition of the composition that if F is compounded of f, f' and if the forms F, f, f' are equivalent respectively, to forms $\bar{F}, \bar{f}, \bar{f}'$, then $\bar{F}$ is compounded of $\bar{f}$ and $\bar{f}'$. This theorem may be reversed (and this is the main property of the composition) as follows: (D. A. [20], art. 239): *if F is compounded of f, f' and $\bar{F}$ of $\bar{f}, \bar{f}'$, and the forms f, f' are equivalent to $\bar{f}, \bar{f}'$, respectively, then F is equivalent to $\bar{F}$.* Thus, the composition is a property of classes and not of separate forms only. Finally, in art. 240, by means of a complicated, masterly performed calculation, Gauss proves the *associativity* of the composition, i.e. that composing three given forms f, f', f'' in one, and then in another order (in other words, $(ff')f''$ and $f(f'f'')$, results in two equivalent forms. The commutativity of the composition follows directly from the definition.

From this short survey of Gaussian theory of the composition it is evident that for a general composition (any two forms whose determinants differ only by a square) this theory involves complicated calculations. Therefore, for frequent everyday application it is useful to have a simplification of the composition, which, although not a very general one, may be performed simply. Such simplification has been given by Dirichlet in his article "De formarum binariarum secundi gradus compositione" ([3], vol. II, p. 105, see also L. Dirichlet [14], § 145 and after). Due to its importance, we shall consider this method in detail.

LEMMA I. *If all determinants of the second order of the matrix*

$$\begin{pmatrix} p_1 & p_2 \dots p_n \\ q_1 & q_2 \dots q_n \end{pmatrix}$$

are divisible by a number m, and if numbers $p_1, \dots, p_n$, m *have no common factor, then there exists a unique solution x modulo m of congruences*

$$p_1 x \equiv q_1, \quad p_2 x \equiv q_2, \quad \dots, \quad p_n x \equiv q_n \pmod{m}.$$

Since the greatest common divisor of numbers $p_1, \dots, p_n$ is relatively prime to m, we can find integers $h_1, \dots, h_n$ satisfying the condition $h_1 p_1 + \dots + h_n p_n \equiv 1 \pmod{m}$. Taking $x \equiv \sum h_i q_i p_k \pmod{m}$ we find for every k, $p_k x \equiv \sum_i h_i p_k q_i \equiv \sum_i h_i q_k \equiv q_k \pmod{m}$ i.e. x satisfies the given congruences, and this solution is unique, modulo m, since $p_1, \dots, p_n$, m have no common factor.

LEMMA II. *If* $b^2 \equiv d \pmod{a}$, $b'^2 \equiv d \pmod{a'}$ *and if numbers* a, a', $b+b'$ *have no common factor, then there exists a unique class of numbers B modulo* aa' *which satisfy the congruences* $B \equiv b \pmod{a}$, $B \equiv b' \pmod{a'}$, $B^2 \equiv d \pmod{aa'}$ *moreover,* a, a' $2B$ *also have no common factor.*

From identity $(B-b)(B-b') = B^2-(b+b')B+bb'$ it is evident that the third congruence for number B (when the first two hold) may be replaced by $(b+b')B \equiv bb'+d \pmod{aa'}$ thus, the number B must satisfy congruences $aB \equiv ab'$, $a'B \equiv a'b$, $(b+b')B \equiv bb'+d \pmod{aa'}$, and the existence of a unique class of such numbers B modulo aa' follows from the previous lemma since the matrix $\begin{pmatrix} a & a' & b+b' \\ ab' & a'b & bb'+d \end{pmatrix}$ satisfies all conditions of the lemma. If a, a' and

$2B$ were divisible by a prime p, then from the first two congruences for B we would have $B \equiv b \equiv b'$, $2B \equiv b+b'$, $b+b' \equiv 0 \pmod{p}$ which is impossible.

Let us call the forms $f = (a, b, c)$ and $f' = (a', b', c')$ of the same determinant d *concordant* (einig) if a, a', $b+b'$ have no common factor. The Dirichlet composition consists of compositions of concordant forms. It follows from lemma II that there exists a series of parallel (§ 9) forms (aa', B, C) (where $C = (B^2-d)/aa'$) of the same determinant d each of which will be called *compounded* of f and f'. Let us note that from congruences for B (Lemma II), it follows that the forms f, f' are parallel (and, consequently, properly equivalent) to forms $\bar{f} = (a, B, a'C), f' = (a', B, aC)$ respectively. The latter forms are also concordant, since a, a', $2B$ have no common factor. It is easy to see that the given definition of a compounded form is in accordance with the Gaussian definition; namely, a substitution

$$X = xx' - Cyy', \quad Y = (ax+By)y' + (a'x'+By')y \tag{30}$$

transforms form $aa'X^2+2BXY+CY^2$ into the product $\bar{f}(x, y)\bar{f}'(x', y')$. The main theorem on composition in the Dirichlet interpretation is formulated as follows: *if two concordant forms* (a, b, c), (a', b', c') *are properly equivalent to two concordant forms* (m, n, l), (m', n', l') *then the form* (aa', B, C) *compounded of two first forms is properly equivalent to form* (mm', N, L) *compounded of two second forms.* It follows from the conditions of the theorem that the forms $(a, B, a'C)$ and $(m, N, m'L)$ are properly equivalent, i.e. that there exists a proper representation x, y of number m by a form $(a, B, a'C)$ belonging to root N of congruence $N^2 \equiv d \pmod{m}$; and this, by Note, § 1, is equivalent to conditions

$$\begin{gathered} ax^2+2Bxy+a'Cy^2 = m, \quad ax+(B+N)y \equiv 0, \\ (B-N)x+a'Cy \equiv 0 \pmod{m}. \end{gathered} \tag{31}$$

Similarly, there exist integers x', y' satisfying the conditions

$$\begin{gathered} a'x'^2+2Bx'y'+aCy'^2 = m', \quad a'x'+(B+N)y' \equiv 0 \\ (B-N)x'+aCy' \equiv 0 \pmod{m'}. \end{gathered} \tag{32}$$

Define integers X, Y in terms of x, y; x', y' by (30). For these X, Y we have

$$\begin{aligned} &aa'X^2+2BXY+CY^2 \\ &\quad = (ax^2+2Bxy+a'Cy^2)(a'x'^2+2Bx'y'+aCy'^2) = mm'. \end{aligned} \tag{33}$$

Further, from congruences (31) and (32) we have

$$\begin{aligned} aa'X+(B+N)Y &= [ax+(B+N)y][a'x'+(B+N)y']+ \\ &\quad +(d-N^2)yy' \equiv 0 \pmod{mm'}, \\ d[(B-N)X+CY] &= [ax+(B+N)y][(B-N)x'+aCy']+ \\ &\quad +(N^2-d)yy' \equiv 0 \pmod{mm'}. \end{aligned} \tag{34}$$

and similarly

$$a'[(B-N)X+CY] \equiv 0, \quad (B-N)[(B-N)X+CY] \equiv 0,$$
$$(B+N)[(B-N)X+CY] \equiv 0 \pmod{mm'},$$

from which, since a, a', $2B$ have no common factor, we have

$$(B-N)X+CY) \equiv 0 \pmod{mm'}. \tag{35}$$

Equality (33) together with congruences (34), (35) express, by the note of § 1, the proper equivalence of the forms (aa', B, C) and (mm', N, L).

To establish what restriction should be imposed on the component classes by the Dirichlet composition, take two concordant forms $f = (a, b, c)$ and $f' = (a', b', c')$ and denote by σ, σ' their divisors. These numbers also divide forms $\bar{f} = (a, B, a'C)$, $f' = (a', B, aC)$ equivalent to f, f'. Since a, a', $2B$ have no common factor, it follows from $a \equiv 2B \equiv 0 \pmod{\sigma}$ that σ is relatively prime to a' and, consequently, to σ'. Therefore, divisors σ, σ' of concordant forms must be relatively prime. We have $a'C \equiv 0 \pmod{\sigma}$, and $(\sigma, a') = 1$, hence $C \equiv 0 \pmod{\sigma}$; similarly we prove that C is divisible by σ', and consequently C is divisible by $\sigma\sigma'$. Thus, numbers aa', $2B$ and C are divisible by $\sigma\sigma'$. If a prime p divides $aa'/\sigma\sigma', 2B/\sigma\sigma', C/\sigma\sigma'$ then it divides either a/σ or a'/σ'. If, for example a/σ is divisible by p, then a, $2B$, $a'C$ are divisible by $p\sigma$, which is impossible since σ is the divisor of the form $\bar{f}$. Hence $\sigma\sigma'$ is the divisor of the form (aa', B, C) compounded of f, f'. Further, let us note that if we are given two classes K, K' of forms of determinant d with relatively prime divisors σ, σ' then we can always select a form f of class K and a form f' of class K' in such a way that these forms are concordant. Let (a'', b'', c'') be any form of class K; since its divisor σ is relatively prime to σ', we can find relatively prime numbers x, y for which $a = a''x^2+2b''xy+c''y^2$ is relatively prime to σ', and form (a'', b'', c'') may be replaced by an equivalent form (a, b, c) whose first coefficient is a. After this, by the same method, we find in

K' a form (a', b', c') with a' relatively prime to a. This form is, clearly, concordant with (a, b, c). Combining these remarks with the main theorem proved above, we can state: the Dirichlet composition enables us to find for every two classes K, K' of determinant d with relatively prime divisors σ, σ' a third class of the same determinant with divisor $\sigma\sigma'$; this class will be called the *product* of classes K and K', and denoted by KK' or $K'K$. In particular, we may compose a properly primitive class $K(\sigma = 1)$ with any other class K'. It is easy to show (L. Dirichlet [14] § 147) that this multiplication is associative, i.e. that for three classes K, K', K'' (whose divisors are pairwise relatively prime) the products $K(K'K'')$, $(KK')K''$ and $(KK'')K'$ denote the same class which we shall denote by $KK'K''$. Clearly, the principal form $(1, 0, -d)$ (§ 8) is concordant with every other form f of determinant d, and, compounding $(1, 0, -d)$ with f, we come to a form parallel to f. Thus, the principal class plays the role of the unit in the multiplication of classes; therefore the principal class will be denoted everywhere, where it does not create confusion, simply by symbol 1. If (a, b, c) is a form of a properly primitive class K, then, clearly, it is concordant with form (c, b, a) and the composition of these two forms leads to form $(ac, b, 1)$. Remembering that (c, b, a) belongs to the opposite class K^{-1} (§ 9), we may say that the product of two opposite classes (properly primitive) is equal to the principal class $KK^{-1} = 1$, in particular, for an ambiguous class we have $KK = K^2 = 1$. From here follows an important corollary: if K is a properly primitive class, and L and L' are any classes, then for $KL = KL'$ we have $L = L'$; to prove this both sides of equality $KL = KL'$ are multiplied by K^{-1}.

Since the multiplication of two properly primitive classes results in a properly primitive class, we may say that h classes of a properly primitive order of a given determinant d form a finite Abelian group (for $d < 0$ we consider a positive order). The study of the structure of this group involves great difficulties and has not advanced since Gauss. If K is any properly primitive class then there exist positive exponents δ for which $K^\delta = 1$; the smallest of these exponents is a divisor of the number of classes h. Let the elements $K_1, K_2, \ldots, K_s$, with exponents $\delta_1, \delta_2, \ldots, \delta_s$ form a basis of the Abelian group under consideration i.e. $K_i^{\delta_i} = 1$ $(i = 1, 2, \ldots, s)$ and as $x_1, \ldots, x_s$ run, independently of each other through complete systems of residues to moduli $\delta_1, \ldots, \delta_s$, $K_1^{x_1}, K_2^{x_2}, \ldots, K_s^{x_s}$ runs just once through all properly primitive

classes, so that $h = \delta_1 \delta_2 \ldots \delta_s$. As is known (H. Weber [93], p. 45) elements K_i of the basis may be chosen in such way that all δ_i are powers of primes, so that the series of numbers δ_i (independent of order) is of the form $p^\alpha, p^\beta, \ldots, p_1^{\alpha_1}, p_1^{\beta_1}, \ldots$, where $p, p_1, \ldots$ are distinct primes, and $0 < \alpha \leqq \beta \leqq \ldots, 0 \leqq \alpha_1 \leqq \beta_1 \leqq \ldots$). The set of such primes (which are called the *invariants* of the group) is completely defined by a given group and, conversely, the invariants completely define the Abelian group. It is easy to show that for a prime p the number of elements K of the group, which satisfy $K^p = 1$, is equal to p^e where e is the number of invariants which are equal to powers of p, i.e. invariants of the form $p^\alpha, p^\beta, \ldots$. For $p = 2$ the classes satisfying $K^2 = 1$ are nothing else but the ambiguous classes; the number of such classes was defined in § 9. Taking into account the result obtained there, we may state the following theorem: *the number of invariants of the group of classes of a properly primitive order of determinant d, which are equal to powers of* 2, *is defined as follows*: $e = (d) - 1$ *for* $d \equiv 1 \pmod 4$, $e = (d)$ *for* $d \equiv 2, 3 \pmod 4$ *or* $d \equiv 4 \pmod 8$ *and* $e = (d) + 1$ *for* $d \equiv 0 \pmod 8$ (*for* $d < 0$ *only the classes of positive forms are considered*). The product of all invariants of the group is equal to the order of the group, i.e. to the number of classes h. Therefore, h is odd if and only if the group has no invariants of the form 2^α, i.e. if and only if the number e defined in the previous theorem is equal to zero. This provides a useful corollary: *the number of classes of a properly primitive order of determinant d* (*positive for* $d < 0$) *is odd if and only if d has one of values* $d = -1, d = \pm 2, d = -4, d = (\pm p)^k$ *where in the last expression p is an odd prime, k is an odd index, and the sign* $\pm$ *is chosen by the condition* $\pm p \equiv 1 \pmod 4$. Let d be a determinant not equal (as usual) to a square, and let $m > 0$ be an integer, relatively prime to $2d$ of which d is a quadratic residue. Taking any root of the congruence $n^2 \equiv d \pmod m$ and assuming $(n^2 - d)/m = l$, we obtain a form $(m, n, l) = f$ of determinant d, positive for $d < 0$. Since $(m, 2n) = 1$ the form f is properly primitive and is concordant with itself. Compounding f with f we obtain a form $f'' = (m^2, n', l')$ of the same determinant d in which $n' \equiv n \pmod m$, consequently $(m, n + n') = (m, 2n) = 1$. Therefore, f'' is concordant with f. Compounding f'' with f we obtain a form $f''' = (m^3, n'', l'')$ etc. Let δ be the exponent of the class of the form f in the group of properly primitive classes of determinant d, then δ is a divisor of number

of the classes h, and the form $f^{(\delta)} = (m^\delta, n^{(\delta-1)}\, l^{(\delta-1)})$ belongs to the principal class. Denoting by $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ the transformation bringing $(1, 0, -d)$ into $f^{(\delta)}$ we have $m^\delta = \alpha^2 - d\gamma^2$. Thus, we obtain the following theorem: *if d is a number which is not a square, but is a quadratic residue of number $m > 0$ which is relatively prime to $2d$, then there exists an exponent $\delta > 0$ for which $m^\delta = x^2 - dy^2$ with relatively prime x, y; this exponent δ is a divisor of the number h of properly primitive (positive for $d < 0$) classes of forms of determinant d.* If d has one of the values given in the previous theorem, then the exponent is *odd* since for such d the number of classes h is odd. The latter theorem has already been used in the study of quadratic residues (§ 3, ch. III).

§ 11. Comparison of numbers of classes whose determinants differ by a square

The theory of composition enables us to compare the number of properly and improperly primitive classes of determinant $d \equiv 1 \pmod 4$ (the only case in which both types of classes exist), and also to determine a relation between the numbers of properly primitive classes of determinants d and ds^2 where s is an integer. For $d < 0$, we consider, as always, only positive classes.

Let d be a given determinant and let σ be one of the possible values of the divisors of the forms of this determinant. (§ 5). In any class K of divisor σ we may, clearly, select a form $(a\sigma, b, c)$ in which $(a, \sigma) = 1$. This form presents the result of composition of two concordant forms $(a, b, c\sigma)$ and (σ, b, ac) of which the first is, clearly, properly primitive, and the second is parallel to the *simplest* form of divisor σ (§ 8). Thus, every class K of divisor σ may be obtained by multiplying the simplest class K_0 of the same divisor by a properly primitive class. Consider the set R of r properly primitive classes H which, when multiplied by K_0 still give class K_0. Since from $K_0 = K_0 H$, $K_0 = K_0 H'$ follows $K_0 HH' = K_0 H' = K_0$ the set R presents a subgroup of the group of properly primitive classes. By a well-known theorem, the order r of this subgroup is a divisor of the order h of the whole group. Splitting the group of properly primitive classes into cosets by means of subgroup R: R, RL_1, RL_2, . . . we easily find that

the simplest class K_0, when multiplied by properly primitive classes belonging to distinct cosets, gives distinct classes of divisor σ. It is clear from this that if h_1 denotes the number of distinct classes of determinant σ, then the ratio h/h_1 is an integer r, which is the order of subgroup R. To find a criterion for a properly primitive class to belong to subgroup R, let us note that in any properly primitive class we may select a form $(a, B, C\sigma)$ in which $(a, \sigma) = 1$, but $2B$ and C are divisible by σ. In fact, taking in the given class a form (a, b, c) where $(a, \sigma) = 1$ we compound it with the simplest form of divisor σ: (σ, b', c'). We obtain a form $(a\sigma, B, C)$ where $2B$ and C are divisible by σ; moreover, by the results of the previous section, form (a, b, c) is equivalent to form $(a, B, C\sigma)$ which may be selected as a representative of the given class.

Now, let H be a given properly primitive class belonging to R i.e. $K_0 H = K_0$. Taking in H a form of a described type $(a, B, \sigma C)$ we find that the form $(a\sigma, B, C)$ from $K_0 H$ is equivalent to the form (σ, B, aC) of K_0; consequently, for integers α, γ we have $a\sigma\alpha^2 + 2B\alpha\gamma + C\gamma^2 = \sigma$ and for $x = \sigma\alpha$, $y = \gamma$ we have $ax^2 + 2Bxy + C\sigma y^2 = \sigma^2$, i.e. a form of class H represents σ^2 (properly or improperly). Conversely, if for integers x, y we have $ax^2 + 2Bxy + C\sigma y^2 = \sigma^2$ then we may show that $x \equiv 0 \pmod{\sigma}$. In fact, if $(x, \sigma) = \delta$, $x = \delta x'$, $\sigma = \delta\sigma'$,, $(x', \sigma') = 1$ then $ax'^2 + (2B/\sigma)\sigma' x'y + (C/\sigma)\sigma'^2 y^2 = \sigma'^2$, ax'^2 is divisible by σ', and, since $(a, \sigma) = 1$, $(x', \sigma') = 1$, we have $\sigma' = 1$, $\delta = \sigma$, $x = \sigma x'$. From $ax'^2 + (2B/\sigma)x'y + (C/\sigma)y^2 = 1$ it is evident that x', y are relatively prime, and that the form $(a\sigma, B, C)$ belonging to class $K_0 H$ is equivalent to the form whose first coefficient is σ, and the latter form is parallel to the simplest form of divisor σ, i.e. $K_0 H = K_0$. Thus, a properly primitive class H belongs to subgroup R if and only if the forms of this class represent number σ^2, properly or improperly. If the form f represents σ^2, then the same form represents *properly* a number δ^2, where δ is a divisor of σ, and hence f is equivalent to a form whose first coefficient is δ^2. Finally, we obtain: the ratio $h/h_1 = r$ is equal to the number of all non-equivalent to each other properly primitive forms of determinant d, first coefficients of which are of the form δ^2 where δ is any divisor of σ. Let us note that in evaluating the number of non-equivalent forms (δ^2, b, c) for every δ, it is sufficient to give to b the values incongruent modulo δ^2, since parallel forms are always equivalent (§ 9).

Let us apply this result to the case $\sigma = 2$, $d \equiv 1 \pmod 4$. In this case $h_1 = h'$ is the number of improperly primitive classes of determinant d, and $\delta^2 = 1$ or 4; in the latter case, the middle coefficient of the form (δ^2, b, c) must be odd. Thus, h/h_1 is equal to the number of non-equivalent properly primitive forms amongst the forms $f_0 = (1, 0, -d), f_{\pm 1} = (4, \pm 1, n)$ where $n = (1-d)/4$. For $d \equiv 1 \pmod 8$ n is even and forms $f_{\pm 1}$ are not properly primitive, hence $h = h'$. For $d \equiv 5 \pmod 8$ all three forms $f_0, f_{\pm 1}$ are properly primitive. To investigate equivalence of the forms the following remarks are useful:

1) If equation $t^2 - du^2 = 4$ is solvable in odd integers t, u then all three forms $f_0, f_{\pm 1}$ are equivalent. In fact, suitably choosing the signs of odd integers t, and using the condition $t+u \equiv 0 \pmod 4$ we may write an integer substitution of determinant 1

$$\begin{pmatrix} t & \pm\dfrac{t+du}{4} \\ \pm u & \dfrac{t+u}{4} \end{pmatrix},$$

transforming f_0 into $f_{\pm 1}$.

2) If any two of the forms $f_0, f_{\pm 1}$ are equivalent, then equation $t^2 - du^2 = 4$ is solvable in odd integers. If f_0 is equivalent to one of the forms $f_{\pm 1} = (4, \pm 1, n)$, then the number 4 is properly representable by form $f_0 = (1, 0, -d)$ from which we obtain $4 = t^2 - du^2$ with odd t, u. If f_{+1} is equivalent to f_{-1} then there exists a proper representation α, γ of number 4 by form f_{+1}, belonging to the root $x = -1$ of congruence $x^2 \equiv d \pmod 4$ (§ 1). For this representation, by (2) § 1, we have $4a^2 + 2\alpha\gamma + n\gamma^2 = 4$, $2\alpha + n\gamma \equiv 0 \pmod 4$, since n is odd, γ is even. Taking $\gamma = 2u$, $2\alpha + u = t$, we obtain $t^2 - du^2 = 4$, $t+u \equiv 0 \pmod 4$ from which it is easy to deduce that numbers t, u are odd. Thus, forms $f_0, f_{\pm 1}$ belong either to one, or to three distinct classes depending on equation $t^2 - du^2 = 4$ being solvable or unsolvable in odd integers; in the first case, we have $h = h'$, in the second $h = 3h'$. For $d < -3$ the only solution of equation $t^2 - du^2 = 4$ is $t = \pm 2$, $u = 0$, consequently, $h = 3h'$; for $d = -3$ we have $t = \pm 1$, $u = \pm 1$, $h = h'$. For $d > 0$ it transpires from (15) § 5, that equation $t^2 - du^2 = 4$ is soluble in odd integers if and only if the *least* solution T, U of this equation consists of odd integers. We obtain the following theorem (Gauss [20] D. A. art. 256):

THEOREM 14. *Let d be an integer of the form $4n+1$, which is not equal to a perfect square, and let h, h' denote the numbers of properly and improperly primitive classes of determinant d, positive for $d < 0$; then for $d < 0$ we have*

$$h = h' \quad \text{if } d \equiv 1 \pmod 8 \text{ or } d = -3;$$
$$h = 3h' \quad \text{for } d \equiv 5 \pmod 8 \text{ and } d < -3;$$

for $d > 0$

$$h = h' \quad \text{if } d \equiv 1 \pmod 8 \text{ or } d \equiv 5 \pmod 8,\ T, U \text{ odd}$$
$$h = 3h' \quad \text{for } d \equiv 5 \pmod 8,\ T, U \text{ even},$$

where T, U is the least solution of equation $t^2 - du^2 = 4$.

There still is no simple rule allowing us to find when the least solution of equation $t^2 - du^2 = 4$ (for d of the form $8k+5$) consists of even numbers T, U and when of odd. There are, for example, only 125 values of d of the form $8k+5$ greater than zero and less than 1000; Out of these 31 numbers T, U are even, and the remaining 94 numbers T, U are odd. The table of these least solutions for all $d \leqq 997$ was computed by Cayley (this table is copied in Grave's [22] textbook).

To deduce further corollaries from the results obtained above (concerning the ratio h/h_1) let us assume that σ is a prime, greater or equal to 2, and $d/\sigma^2 = d'$ is an integer. Then h_1 is, clearly, equal to the number of properly primitive classes of determinant d'. To determine h/h_1 we must, according to the above, evaluate how many classes originate from the forms $g = (1, 0, -d)$ and $f_b = (\sigma^2, b\sigma, b^2 - d')$. In the latter form b runs through a complete system of residues modulo σ, except the solutions of a congruence $b^2 \equiv d' \pmod \sigma$ (if such solutions exist); under this condition all forms f_b are properly primitive. The number l of forms g, f_b is equal to 2 for $\sigma = 2$, and to $\sigma - (d'/\sigma)$ for odd σ (assuming the Legendre's symbol $(d'/\sigma) = 0$ when d' is divisible by σ). The study of equivalence of forms g, f_b is based on the following propositions:

1) Form g is equivalent to a form f_b if and only if equation $t^2 - d'u^2 = 1$ is solvable in integers t, u satisfying the condition $t + bu \equiv 0 \pmod \sigma$. In fact, by (2), § 1, g and f_b are equivalent if and only if there exist integers x, y for which $x^2 - d'\sigma^2 y^2 = \sigma^2$, $x + b\sigma y \equiv 0$ $-b\sigma x - d'\sigma^2 y \equiv 0 \pmod{\sigma^2}$. Clearly x is divisible by σ; taking $x = \sigma t$, $y = u$ we obtain $t^2 - d'u^2 = 1$, $t + bu \equiv 0 \pmod \sigma$.

2) Forms f_b and $f_{b'}$ are equivalent if and only if equation $t^2-d'u^2 = 1$ has a solution satisfying the condition $(b-b')t+(bb'-d')u \equiv 0 \pmod{\sigma}$. In fact, the equivalence of f_b and $f_{b'}$ is equivalent to the existence of integers x, y for which $\sigma^2x^2+2b\sigma xy+(b^2-d')y^2 = \sigma^2$, $\sigma^2x+(b+b')\sigma y \equiv 0$, $(b-b')\sigma x+(b^2-d')y \equiv 0 \pmod{\sigma^2}$. Since b^2-d' is not divisible by σ, we have $y = \sigma u$, u an integer; taking also $x = t-bu$, we arrive at the above conditions of equivalence of forms f_b and $f_{b'}$.

Suppose that among forms g, f_b there exist just λ forms belonging to the principal class (i.e. equivalent to g) and let us prove that the ratio $h/h_1 = r$ is equal to the total number l of forms g, f_b, divided by λ. First, let us note that among forms f_b there exists, by supposition, $\lambda-1$ forms of the principal class; to every such form f_b corresponds by 1) a number b satisfying $t+bu \equiv 0 \pmod{\sigma}$ for some solution, t, u of equation $t^2-d'u^2 = 1$. Obviously, in this solution $u \not\equiv 0 \pmod{\sigma}$. Conversely, to every solution, t, u of equation $t^2-d'u^2 = 1$ with $u \not\equiv 0 \pmod{\sigma}$ corresponds a definite residue b modulo σ, defined by congruence $t+bu \equiv 0 \pmod{\sigma}$, and, consequently, to every such solution corresponds a form f_b belonging to the principal class. Therefore, $\lambda-1$ represents the number of distinct residues $-t/u \pmod{\sigma}$ originating from various solutions of equation $t^2-d'u^2 = 1$ with $u \not\equiv 0 \pmod{\sigma}$. Equality $r = 1/\lambda$ will be proved if we show that to every form $f_{b'}$ which does not belong to the principal class, (if such a form exsits), there corresponds among forms f_b just $\lambda-1$ forms distinct from it and equivalent to it. In fact, if $f_b \sim f_{b'}$, and if f_b is distinct from $f_{b'}$, i.e. $b \not\equiv b' \pmod{\sigma}$, then by proposition 2) for some solution of equation $t^2-d'u^2 = 1$ we have $(b-b')t+(bb'-d')u \equiv 0 \pmod{\sigma}$. Since $u \not\equiv 0$, we obtain, on defining β from the congruence $\beta \equiv -t/u \equiv (bb'-d)/(b-b') \pmod{\sigma}$, a form f_β equivalent to g.

Thus, to every form f_b, distinct from $f_{b'}$ and equivalent to $f_{b'}$, there corresponds, in the sequence of forms f, a form f_β belonging to the principal class; the suffix β is defined by the suffixes b, b' from the congruence $(b-b')\beta \equiv bb'-d' \pmod{\sigma}$.

Conversely, let a form $f_\beta \neq g$ be given; using β and b' to define the number b by means of congruence $(\beta-b')b \equiv \beta b'-d'$ where, clearly, $\beta \not\equiv b' \pmod{\sigma}$, we show that $f_b \sim f_{b'}$ and $f_b \neq f_{b'}$. First (to prove the existence of a form f_b corresponding to b) we must verify that $b^2 \not\equiv d' \pmod{\sigma}$. In fact, if the opposite were true, we

would have $(\beta-b')b \equiv \beta b'-b^2$, $(b-b')(\beta+b) \equiv 0$, i.e. either $\beta^2 \equiv d'$ or $b'^2 \equiv d' \pmod{\sigma}$ which is impossible. If we had $f_b = f_{b'}$, i.e. $b \equiv b' \pmod{\sigma}$ then from the congruence for b we have $b'^2 \equiv d' \pmod{\sigma}$. Since $f_\beta \sim g$ then, by proposition 1 there exists a solution of equation $t^2-d'u^2 = 1$ for which $\beta \equiv -1/u \pmod{\sigma}$ which, together with congruences for b gives

$$(b-b')t+(bb'-d)u \equiv 0, \qquad \text{i.e. } f_b \sim f_{b'},$$

q.e.d. If $d' < 0$ then for $d' \neq -1$ equation $t^2-d'u^2 = 1$ has only two solutions $t = \pm 1$, $u = 0$; for $d' = -1$ two more are adjoined to them: $t = 0$, $u = \pm 1$. In the first case we have $\lambda = 1$, in the second case $\lambda = 2$; therefore, for $d' < 0$ the ratio h/h_1 is, in general equal to l and only for $d' = -1$ it is equal to $\frac{1}{2}l$. If $d' > 0$, then we note that two solutions t_1', u_1' and t', u' of equation $t'^2-d'^2u'^2 = 1$ with u_1' and $u' \not\equiv 0 \pmod{\sigma}$ give one residue $\beta \equiv -t_1'/u_1' \equiv -t'/u' \pmod{\sigma}$ if and only if the ratio $(t_1'+u_1'\sqrt{d'})/(t'+u'\sqrt{d'}) = (t_1'+u_1'\sqrt{d'})(t'-u'\sqrt{d'})$ may be represented in a form $t+u\sqrt{d}$ where t, u is a solution of $t^2-du^2 = 1$. Let us distribute all solutions of equation $t'^2-d'u'^2 = 1$ into groups, referring to each group two solutions t_1', u_1'; t', u' for which $t_1'+u_1'\sqrt{d'} = (t'+u'\sqrt{d'})(t+u\sqrt{d})$ where t, u are solutions of equation $t^2-du^2 = 1$; the number of these groups is, clearly, equal to λ. Denoting, on the other hand, by T, U; T', U' the least positive solutions of equations $t^2-du^2 = 1$, $t^2-d'u'^2 = 1$ and by μ the integral exponent in equation $T+U\sqrt{d} = (T'+U'\sqrt{d'})^\mu$. (cf. end of § 5), we see that solutions $t_1'+u_1'\sqrt{d'} = \pm(T'+U'\sqrt{d'})^a$ and $t'+u'\sqrt{d'} = \pm(T'+U'\sqrt{d'})^b$ belong to the same group if and only if $a \equiv b \pmod{\mu}$. Thus, $\lambda = \mu$ and the ratio h/h_1 for $d > 0$ may be expressed as

$$\frac{h}{h_1} = \frac{1}{\lambda} = l\,\frac{\log(T'+U'\sqrt{d'})}{\log(T+U\sqrt{d})}.$$

Applying the above results several times in succession we finally obtain the following theorem: (Gauss [20], D. A. art. 256. L. Dirichlet [14] § 151):

THEOREM 15. *If $h(d)$ is the number of properly primitive classes of determinant d which is not a square, where the classes are positive if $d < 0$ and $s \geqq 0$ is an integer, then*

$$h(ds^2) = h(d) \cdot \varepsilon s \prod \left(1 - \left(\frac{d}{r}\right) \cdot \frac{1}{r}\right),$$

where the product is taken over all distinct prime divisors r of number s, and Legendre symbol (d/r) *is equal to zero for d divisible by r;* $\varepsilon = 1$ *for* $d < -1$ *and* $\varepsilon = \frac{1}{2}$ *for* $d = -1$, $s \geqq 1$. *Finally, for* $d > 0$,

$$\varepsilon = \frac{\log(T' + U'\sqrt{d'})}{\log(T + U\sqrt{d})},$$

where T, U; T', U' *are the least positive solutions of equations* $t^2 - ds^2u^2 = 1$, $t'^2 - du'^2 = 1$.

Another elementary proof of the theorems of the present section was proposed by Lipschitz (see L. Dirichlet [14], p. 254).

§ 12. Distribution of binary forms into genera

We have seen in § 10, that the classes of a properly primitive order of a given determinant constitute an abelian group. If we assign to every class K a number $\chi(K)$, having the properties $\chi(1) = 1$, $\chi(KK') = \chi(K)\chi(K')$, for every two classes K, K', then $\chi(K)$ is the *character* of the group of classes (Weber [93], p. 49); determining these characters is equivalent to determining the structure of the group. The values of the function $\chi(K)$ are, clearly, the roots of unity, i.e. generally speaking they are complex numbers. Gauss's study of the *theory of genera* (Genera formarum, D. A. [20] art. 228 and the following) presents nothing else but the definition of all the *real* characters of an abelian group of classes, i.e. such characters $\chi(K)$ whose values are equal to ± 1. In a simpler form this theory is set forth by Dirichlet [14] (Suppl. IV and X).

Let $f(x, y) = ax^2 + 2bxy + cy^2$ be a properly or improperly primitive form of determinant d, let p be any odd prime divisor of d, and let $n = f(\alpha, \gamma)$, $n' = f(\beta, \delta)$ be two numbers represented by form f and not divisible by p. Substitution $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ with determinant $\alpha\delta - \beta\gamma = e$, transforms f into a form (n, l, n') where $l^2 - nn' = de^2$, from which $l^2 \equiv nn' \pmod{p}$, $(n/p) = (n'/p)$. Thus, the symbol (n/p) has the same value for all numbers $n \not\equiv 0 \pmod{p}$ representable by form f; this symbol $(n/p) = \chi(n) = \chi(f)$ will be called the *generic*

character of form f. The value of $\chi(f)$ may always be determined by means of the first and last coefficients a, c of form f, which belong to the set of integers representable by f and at least one of which is not divisible by p (since f is a primitive form by supposition). Further, every form f' equivalent to f represents the same numbers as f so that $\chi(f') = \chi(f)$. Thus, the quantity $(n/p) = \chi(f)$ depends only on the *class* K of form f and may therefore be denoted thus: $\chi(K)$. If $p_1, p_2, \ldots, p_\nu$ are all distinct prime divisors of d, then we define ν values $\chi_i(f) = (n/p_i)$ $(i = 1, 2, \ldots, \nu)$. If $d \equiv 1 \pmod 4$ there are no more such values. Otherwise the supplementary characters are defined as follows: Let $d \equiv 3 \pmod 4$ (so that f is a *properly* primitive form) and let n and n' be two odd numbers representable by form f. From $l^2 - nn' = de^2$ we obtain $nn' \equiv l^2 + e^2 \pmod 4$ and since integers l, e are of different parity, we have $nn' \equiv 1$, $n' \equiv n \pmod 4$. Therefore, the unit $\chi_{\nu+1}(n) = (-1)^{\frac{1}{4}(n-1)}$ remains unaltered for all odd numbers n representable by form f. Similarly we show (L. Dirichlet [14] § 41) that the same property is possessed by $\chi_{\nu+1}(n) = (-1)^{\frac{1}{8}(n^2-1)}$ for $d \equiv 2 \pmod 8$, $\chi_{\nu+1}(n) = (-1)^{\frac{1}{8}(n^2-1)+\frac{1}{4}(n-1)}$ for $d \equiv -2 \pmod 8$, $\chi_{\nu+1}(n) = (-1)^{\frac{1}{4}(n-1)}$ for $d \equiv 4 \pmod 8$, finally $\chi_{\nu+1}(n) = (-1)^{\frac{1}{4}(n-1)}$ and $\chi_{\nu+2}(n) = (-1)^{\frac{1}{8}(n^2-1)}$, for $d \equiv 0 \pmod 8$. All these quantities are generic characters of form f and its class K. If K, K' are two classes of which one or both are properly primitive, then choosing in K and K' concordant forms with first coefficients a and a' relatively prime to d (or $2d$), the first coefficient of the form compounded of them is equal to aa', from which $\chi_i(KK') = \chi_i(K)\chi_i(K')$; Further, the principal form $f_0 = (1, 0, -d)$ it is clear that $\chi_i(f_0) = 1$. Thus, all introduced quantities $\chi_i(K)$ do, in fact, possess properties of characters.

Consider all classes of a properly or improperly primitive order of determinant d, positive for $d < 0$. For every such class K the above characters $\chi_1(K)$, $\chi_2(K), \ldots$ (whose number is equal to $\nu = (d)$ for $d \equiv 1 \pmod 4$, $\nu = (d)+1$ for $d = 2, 3, 4, 6, 7 \pmod 8$, and $(d)+2$ for $d \equiv 0 \pmod 8$, where (d) denotes the number of distinct odd primes dividing d), have a completely determined system of values. The totality of all classes for which this system of values is the same is called the *genus*. (Genus, Geschlecht);. The genus which contains the principal class is called the *principal* genus. (The system of characters corresponding to it is, clearly, $+1, +1, \ldots$). In an im-

properly primitive order the principal genus is the genus containing the primitive form $(2, 1, \frac{1}{2}(1-d))$. The corresponding system of values of characters is $(2/p_1)$, $(2/p_2)$, ... Clearly, the classes of the principal genus G form a subgroup inside the whole group H of properly primitive classes. The remaining genera G_1, G_2, . . . of a properly primitive order are cosets in the coset expansion of H with respect to subgroup G. In particular, it follows from here that all genera contain the same number of classes. The latter conclusion is also true for an improperly primitive order, since by the reasonings of the previous section, multiplication of the simplest improperly primitive class K_0 by all the classes of group H gives all improperly primitive classes (each of them either once, or three times).

The μ characters obtained above are not independent. They have one relationship which may be easily deduced by means of the quadratic reciprocity law. Let f be a properly primitive form of determinant d, and let m be an integer, properly representable by this form and relatively prime to $2d$ (for $d < 0$, $m > 0$). Then f is equivalent to the form (m, l, n) so that $l^2 - mn = d$ and $(d/m) = 1$. Separating in d the highest power of 2, and then applying the reciprocity law to Jacobi symbol in its usual form (which can be done by § 9, ch. I, since of two numbers d, m at least one is greater than zero), we find that every properly primitive class K satisfies a relation:

$$\chi'(K)\chi''(K)\chi'''(K)\ldots = +1. \tag{36}$$

In the left hand side of this formula enter the characters $\chi(K) = (m/p)$, corresponding to all odd primes p, entering into d with *odd* power; moreover, for $d \equiv -2^\alpha \pmod{2^{\alpha+2}}$ ($\alpha \geqq 0$ and even) it contains character $\chi = (-1)^{\frac{1}{2}(m-1)}$, for $d \equiv 2^\alpha \pmod{2^{\alpha+2}}$ ($\alpha > 0$ and odd) it contains the character $\chi = (-1)^{\frac{1}{8}(m^2-1)}$; for $d \equiv -2 \pmod 8$ it contains character $\chi = (-1)^{\frac{1}{8}(m^2-1)+\frac{1}{2}(m-1)}$ and finally for $d \equiv -2^\alpha \pmod{2^{\alpha+2}}$ ($\alpha \geqq 3$, odd) it contains two characters $\chi' = (-1)^{\frac{1}{8}(m^2-1)}$ and $\chi'' = (-1)^{\frac{1}{2}(m-1)}$. Since d (as usual) is assumed not to be equal to a square, it is easy to see that relation (36) is not an identity, i.e. its left hand side contains at least one character. Similarly, we find that for every improperly primitive class K (positive for $d < 0$), the following relation holds:

$$\chi'(K)\chi''(K)\chi'''(K)\ldots = \left(\frac{2}{d}\right). \tag{37}$$

In the left hand side are the characters $\chi(K) = (m/p)$ corresponding to all odd primes p which enter into determinant d with an *odd* power. Since every character χ_i may only take the values ± 1 and since they are connected either by relation (36) or (37), we can *a priori* think of $2^{\mu-1}$ possible systems of values of characters $\chi_1(K), \chi_2(K), \ldots, \chi_\mu(K)$. The question: does each of $2^{\mu-1}$ systems of values answer to a really existing genus in a properly or improperly primitive order, is solved by the following important theorem of Gauss (D.A. [20], art. 287):

THEOREM 16. *Given a properly or improperly primitive order of forms of a non-square determinant d, positive for $d<0$. Let $\chi_i(K)\,(i=1,2,\ldots\mu)$. be the generic characters of this order, where $\mu = (d)$ for $d \equiv 1 \pmod 4$ $\mu = (d)+1$ for $d \equiv 2, 3, 4, 6, 7 \pmod 8$ and $\mu = (d)+2$ for $d \equiv 0 \pmod 8$, where (d) denotes the number of distinct odd prime divisors of d. Then there exists a class K of forms in this order, satisfying system of equations*

$$\chi_1(K) = \varepsilon_1, \quad \chi_2(K) = \varepsilon_2, \ \ldots, \ \chi_\mu(K) = \varepsilon_\mu,$$

(where $\varepsilon_1, \ldots, \varepsilon_\mu$ are given units ± 1), only if the right hand sides of these equations satisfy relation (36) *for properly and* (37) *for improperly primitive order. In other words, the number of genera in a given order is equal to $2^{\mu-1}$.*

Proofs of this theorem were given by Gauss (D.A. [20], art. 287), Dirichlet ([14] § 158) and Arndt; they all use, to certain extent, the theory of ternary forms (see § 15). First of all, let us note that it is sufficient ot prove the theorem for a properly primitive order, since from this we deduce by composition that it is also true for an improperly primitive order. Denoting by h the number of all properly primitive classes, by g the number of classes in every genus, and by e the number of genera, we have, by above, $h = ge$. Consider, on the other hand, the classes which are *squares* of properly primitive classes, and let us denote the number of distinct classes of such kind by $\bar{g}$. It follows from $K^2 = K'^2$ (K, K' are properly primitive classes) that $(K'K^{-1})^2$ i.e. $K'K^{-1} = A$ is an ambiguous class (§§ 4, 10) and hence, remembering the results of § 9, the number of ambiguous classes, is equal to $2^{\mu-1}$, and we may write $h = 2^{\mu-1}\bar{g}$. Since $e \leqq 2^{\mu-1}$ we find from $2^{\mu-1}\bar{g} = eg$ that $\bar{g} \leqq g$, i.e. the number of distinct classes K^2 does not exceed the number of classes in the principal genus. Noting that the square of a class always does belong to the principal genus, we may say

that theorem 16 (expressed by equality $e = 2^{\mu-1}$) is equivalent to the following statement: *every class of the principal genus is a square of some class.* In this form this theorem will be proved in § 15. Theorem 16 implies that the generic characters $\chi_1, \ldots, \chi_\mu$ apart from a single character entering (36) give the *complete* system of independent distinct characters of the group of classes of a properly primitive order.

Let $f = (a, b, c)$ be a given form of determinant $d = b^2 - ac$ and let Δ be a given number. In the theory of ternary forms, we consider a system of congruences

$$\Delta a \equiv M^2, \quad \Delta b \equiv MN, \quad \Delta c \equiv N^2 \pmod{d} \tag{38}$$

in unknowns M, N. We must answer the following questions concerning this system: 1) for what Δ for a given form f does system (38) allow solutions and what is their number? (i.e. the number of systems of integers M, N distinct modulo d, satisfying (38)). 2) What values does Δ take for given d in order that there exist forms f of determinant d for which system (38) has solutions, and what are the forms f? These questions are closely connected with the theory of genera; numbers Δ for which system (38) allows solutions are called characteristic numbers of form f (Gauss [20], D.A. art. 233). We restrict ourselves to the case $(\Delta, d) = 1$ and of a positive form f (for $d < 0$). Under these suppositions, for system (38) to be possible, it is necessary for f to be *primitive*. In fact, taking $\Delta a = M^2 + Pd$, $\Delta b = MN + Qd$, $\Delta c = N^2 + Rd$ (P, Q, R are integers) and eliminating a, b, c from equation $b^2 - ac = d$ we obtain

$$\Delta^2 = -PN^2 - RM^2 + 2QMN + (Q^2 - PR)d \tag{39}$$

If a, b, c were divisible by a prime p, then by (38), (39) M, N and Δ are divisible by p, which contradicts the supposition $(\Delta, p) = 1$. Assuming f to be primitive, and factorising d into prime factors $d = \pm 2^\alpha p_1^{\alpha_1} \ldots p_\nu^{\alpha_\nu}$ (where $\alpha \geqq 0$, $\alpha_1 > 0, \ldots, \alpha_\nu > 0$, $p_1, \ldots, p_\nu$ are odd primes) we find by the general rule (§ 4, ch. I), that system (38) is equivalent to a series of such systems moduli $2^\alpha, p_1^{\alpha_1}, \ldots, p_\nu^{\alpha_\nu}$ and the product of the number of solutions of these systems is equal to the required number of solutions of system (38). The number p_1 cannot divide both numbers a, c; if, for example, $a \not\equiv 0 \pmod{p_1}$ then for a congruence $\Delta a \equiv M^2 \pmod{p_1^{\alpha_1}}$ to be solvable, it is necessary and sufficient that $(a/p_1) = (\Delta/p_1)$. But (a/p_1) is nothing else but the generic character $\chi_1(f)$ of form f; condition $\chi_1(f) = (\Delta/p_1)$

may be expressed by saying that Δ is *concordant* with the character χ_1 of form f. Under this condition congruence $\Delta a \equiv M^2 \pmod{p_1^{\alpha_1}}$ is satisfied by two numbers M distinct modulo $p_1^{\alpha_1}$. (§ 9, ch. I). For each of these, we define N by the condition $N \equiv \Delta b/M \pmod{p_1^{\alpha_1}}$ and obtain $N^2 \equiv \Delta^2 b^2/M^2 \equiv \Delta^2 ac/\Delta a \equiv \Delta c \pmod{p_1^{\alpha_1}}$ so that system (38) has two solutions modulo $p_1^{\alpha_1}$. Further, considering system (38) to modulus 2^α, we see that for $\alpha = 0$, 1 this system is always solvable; for $\alpha = 2$ we must have $\Delta a \equiv 1 \pmod 4$ (assuming a to be odd), and $(-1)^{\frac{1}{2}(a-1)} = \chi_{\nu+1}(f) = (-1)^{\frac{1}{2}(\Delta-1)}$ (i.e. Δ is concordant with the character $\chi_{\nu+1}$ of form f) for $\alpha \geqq 3$, Δ is concordant with characters $\chi_{\nu+1}(f) = (-1)^{\frac{1}{2}(a-1)}$ and $\chi_{\nu+2}(f) = (-1)^{\frac{1}{8}(a^2-1)}$; when these conditions are satisfied, system (38) has 2 solutions for $\alpha = 2$, and four solutions for $\alpha \geqq 3$ to modulus 2^α (§ 9, ch. 1). Thus, for a number Δ to be a characteristic number of a primitive form f, it is necessary and sufficient that this number is concordant: for $d \not\equiv 0 \pmod 4$ with generic characters of f corresponding to *odd* prime factors of d, and for $d \equiv 0 \pmod 4$, with all the generic characters of f, under these conditions the number of solutions of system (38) is equal $2^{(d)}$, $2^{(d)+1}$ or $2^{(d)+2}$ according as $d \not\equiv 0 \pmod 4$, $d \equiv 4 \pmod 8$ or $d = 0 \pmod 8$ respectively.

To answer the second question posed above, let us take into account relations (36) and (37) between the generic characters. Substituting into them, instead of $\chi'(f)$, $\chi''(f)$, ... the values (Δ/p), $(-1)^{\frac{1}{2}(\Delta-1)}$, ... equal to them, we find for $d \equiv 1 \pmod 4$ that $(\Delta/d) = 1$ for a properly primitive form f, and $(2\Delta/d) = 1$ for improperly primitive form f. Δ must satisfy such a condition in order that it is a characteristic number of a primitive form of determinant $d \equiv 1 \pmod 4$; under these conditions we conclude, by theorem 16, that there exists one genus of properly or improperly primitive forms for which Δ is a characteristic number. Similarly, for $d \equiv 0 \pmod 4$ we deduce from (36) that $(d/\Delta) = (\Delta, d)$ where $(\Delta, d) = -1$ for $\Delta < 0$, $d < 0$ and $= +1$, if at least one of numbers a, Δ is greater than zero. In cases when $d \equiv 2, 3 \pmod 4$, relation (36) does not impose any restriction on Δ, i.e. every number Δ, relatively prime to d, is a chacteristic number of some properly primitive forms of determinant d (contained in one definite genus). In fact, in these cases relation (36) contains character $\chi_{\nu+1}(f) = (-1)^{\frac{1}{8}(a^2-1)}$, $(-1)^{\frac{1}{8}(a^2-1)+\frac{1}{2}(a-1)}$ or $(-1)^{\frac{1}{2}(a-1)}$ whose values is determined by the values of characters

$\chi_i(f) = (a/p_i)$, corresponding to odd prime factors p_i of d. Assuming for every p_i that $\chi_i(f) = (\Delta/p_i)$, we determine the required genus of forms f, for which Δ is a characteristic number.

Apply these reasonings to the case when $\Delta = -1, d = -n < 0$. Clearly, the conditions $(\Delta/d) = 1$ and $(d/\Delta) = (\Delta, d)$ for $d \equiv 1$ and $0 \pmod 4$ are not satisfied, whilst the condition $(2\Delta/d) = 1$ (for an improperly primitive order) is satisfied only for $d \equiv 5 \pmod 8$ Thus, *the number* -1 *is a characteristic number of positive forms of determinant* $-n$ *only for* $n \equiv 1, 2 \pmod 4$ *or for* $n \equiv 3 \pmod 8$. *In the first case there exists one genus of properly primitive forms, in the second case – one genus of improperly primitive forms, for which* -1 *is a characteristic number. In both cases the genus is determined by the values of characters* $\chi_i(f) = (-1/p_i)$ *where* p_i *are all odd prime divisors of* n. The result will be used later (§ 16).

§ 13. Ternary forms, finiteness of the number of classes. Basic problems of the theory

The simplest generalisation of binary forms are *ternary* forms, i.e. expressions of the form

$$ax^2+by^2+cz^2+2dxy+2cxz+2gyz \tag{40}$$

in three variables x, y, z. The study of these forms was originated by Lagrange and Legendre, whose investigations of the indefinite equation $ax^2+by^2+cz^2 = 0$ are essentially related to the theory of ternary forms (see Legendre [39], part I § 4). The general basis of the theory was founded by Gauss (D.A. [20], art. 266–300).

Ternary form (40) will be denoted by a matrix

$$A = \begin{pmatrix} a & d & e \\ d & b & g \\ e & g & c \end{pmatrix}.$$

The determinant of this matrix will be called the determinant of the ternary form. Coefficients a, b, c (called the diagonal coefficients) and d, e, g are assumed to be integers. Let the variables x, y, z be transformed into new variables x', y', z' by a linear substitution

$$\begin{aligned} x &= \alpha x'+\beta y'+\gamma z' \\ y &= \alpha' x'+\beta' y'+\gamma' z' \\ z &= \alpha'' x'+\beta'' y'+\gamma'' z' \end{aligned} \tag{41}$$

then the form (40) is transformed into a new ternary form

$$a'x'^2+b'y'^2+c'z'^2+2d'x'y'+2e'x'z'+2g'y'z'. \tag{42}$$

If we denote by A_1 the matrix of this new form and write substitution S of (41) in a matrix form

$$S=\begin{pmatrix}\alpha & \beta & \gamma\\ \alpha' & \beta' & \gamma'\\ \alpha'' & \beta'' & \gamma''\end{pmatrix}$$

then, as is known from algebra, there is a relationship between A and A_1, namely $A_1 = S'AS$ where S' denotes the *transposed* matrix

$$S'=\begin{pmatrix}\alpha & \alpha' & \alpha''\\ \beta & \beta' & \beta''\\ \gamma & \gamma' & \gamma''\end{pmatrix}.$$

This gives the dependence between the determinants Δ and Δ' of forms (40) and (42): $\Delta' = \Delta k^2$ where k is the determinant of the substitution S. It is useful to have formulae expressing implicitly the coefficients of the transformed form (42); denoting the original form (40) by $f(x, y, z)$, we may write these formulae as follows (V. A. Markov [57], p. 13).

$$a' = f(\alpha, \alpha', \alpha''),\quad b' = f(\beta, \beta', \beta''),\quad c' = f(\gamma, \gamma', \gamma''),$$

$$\begin{aligned}
d' &= \frac{1}{2}\frac{\partial f(\alpha, \alpha', \alpha'')}{\partial \alpha}\beta+\frac{1}{2}\frac{\partial f(\alpha, \alpha', \alpha'')}{\partial \alpha'}\beta'+\frac{1}{2}\frac{\partial f(\alpha, \alpha', \alpha'')}{\partial \alpha''}\beta''\\
&= \frac{1}{2}\frac{\partial f(\beta, \beta', \beta'')}{\partial \beta}\alpha+\frac{1}{2}\frac{\partial f(\beta, \beta', \beta'')}{\partial \beta'}\alpha'+\frac{1}{2}\frac{\partial f(\beta, \beta', \beta'')}{\partial \beta''}\alpha'',\\
e' &= \frac{1}{2}\frac{\partial f(\alpha, \alpha', \alpha'')}{\partial \alpha}\gamma+\frac{1}{2}\frac{\partial f(\alpha, \alpha', \alpha'')}{\partial \alpha'}\gamma'+\frac{1}{2}\frac{\partial f(\alpha, \alpha', \alpha'')}{\partial \alpha''}\gamma'' \qquad (43)\\
&= \frac{1}{2}\frac{\partial f(\gamma, \gamma', \gamma'')}{\partial \gamma}\alpha+\frac{1}{2}\frac{\partial f(\gamma, \gamma', \gamma'')}{\partial \gamma'}\alpha'+\frac{1}{2}\frac{\partial f(\gamma, \gamma', \gamma'')}{\partial \gamma''}\alpha'',\\
g' &= \frac{1}{2}\frac{\partial f(\beta, \beta', \beta'')}{\partial \beta}\gamma+\frac{1}{2}\frac{\partial f(\beta, \beta', \beta'')}{\partial \beta'}\gamma'+\frac{1}{2}\frac{\partial f(\beta, \beta', \beta'')}{\partial \beta''}\gamma''\\
&= \frac{1}{2}\frac{\partial f(\gamma, \gamma', \gamma'')}{\partial \gamma}\beta+\frac{1}{2}\frac{\partial f(\gamma, \gamma', \gamma'')}{\partial \gamma'}\beta'+\frac{1}{2}\frac{\partial f(\gamma, \gamma', \gamma'')}{\partial \gamma''}\beta''.
\end{aligned}$$

The definitions of the equivalence of forms, of one form containing the other, and of the class of forms (§ 3, ch. II, §§ 1, 3, ch. IV) still hold for ternary forms; let us note only that here there is no need to distinguish between the proper and improper equivalence, since if a ternary form f is transformed into a ternary form f' by means of integer substitution S of determinant $+1$, then the substitution $-S$(whose coefficients differ from those of S by sign) has determinant -1 and also transforms f into f'.

Replacing in matrix A of form (40) every element by its cofactor, we obtain the matrix

$$A = \begin{pmatrix} a_1 & d_1 & e_1 \\ d_1 & b_1 & g_1 \\ e_1 & g_1 & c_1 \end{pmatrix},$$

which is called adjoint with respect to A; the corresponding ternary form also is called adjoint with respect to form (40). Coefficients of the adjoint form are

$$a_1 = bc-g^2, \quad b_1 = ac-e^2, \quad c_1 = ab-d^2,$$
$$d_1 = eg-dc, \quad e_1 = dg-be, \quad g_1 = de-ag.$$

The determinant of an adjoint form is, clearly, equal to the determinant of the original form. Denoting by Δ the determinant of matrix A, we have, for the adjoint matrix $\bar{A} = \Delta A'^{-1}$ where $'$ and $^{-1}$ are the signs of the transposed and the inverse matrix, and the factor Δ denotes, as usual, multiplication of every element of the matrix by Δ. Hence $\bar{\bar{A}} = \Delta A$ and the adjoint of an adjoint form is the original form multiplied by a square of its determinant. Let a ternary form with matrix A be transformed by substitution S of determinant k into a ternary form with matrix A_1. Passing to conjugate and inverse matrices in the expression $A_1 = S'AS$ we easily obtain $\bar{A}_1 = \bar{S}'\bar{A}\bar{S}$. Calling the substitution with matrix $\bar{S}$ adjoint with substitution S we can say: If a ternary form f is transformed by substitution S into f', then the form F adjoint with f is transformed by adjoint substitution $\bar{S}$ into form F' which is adjoint to f'. Thus, if two ternary forms are equivalent, then their adjoint forms are also equivalent.

Ternary form (40) is called primitive if coefficients a, b, c, d, e, g have no common factor; it is *properly primitive* if at least one of the diagonal coefficients a, b, c is odd, and *improperly primitive* if they are

all even. It is clear from (43) that these properties are not affected in passing over to an equivalent form.

A ternary form f (see (40)) of determinant Δ is called *positive* if for all values of variables x, y, z, not identically zero, $f > 0$; it is called *negative* if $f < 0$ for all such values x, y, z; in all other cases f is called *indefinite*. The conditions for positiveness are, as we know

$$a > 0, \quad c_1 = ab - d^2 > 0, \quad \Delta > 0$$

the conditions for negativeness are

$$a < 0, \quad c_1 = ab - d^2 > 0, \quad \Delta < 0.$$

These properties are also preserved in passing over to equivalent forms. For ternary forms the following important theorem holds, equivalent to theorem 13 for binary forms. (Gauss [20] D.A. art. 276):

THEOREM 17. *All integral ternary forms of a given determinant Δ split into a finite number of classes.*

To prove this theorem a usual method is employed. Namely we prove that: 1) every ternary form is equivalent to some special form which may be called reduced; 2) the number of reduced forms is finite for a given Δ. Let f be a given ternary form and let F be a form adjoint to it, whose matrices are, respectively $\begin{pmatrix} a & d & e \\ d & b & g \\ e & g & c \end{pmatrix}$ and $\begin{pmatrix} A & D & E \\ D & B & G \\ E & G & C \end{pmatrix}$. Transforming f by a substitution $\begin{pmatrix} \alpha & \beta & 0 \\ \gamma & \delta & 0 \\ 0 & 0 & 1 \end{pmatrix}$, $\alpha\delta - \beta\gamma = \pm 1$ whose adjoint substitution is $\begin{pmatrix} \delta & -\gamma & 0 \\ -\beta & \alpha & 0 \\ 0 & 0 & +1 \end{pmatrix}$ and denoting by dashes the coefficients of transformed forms, we obtain, by (43)

$$a' = a\alpha^2 + 2d\alpha\gamma + b\gamma^2 \quad d' = a\alpha\beta + d(\alpha\delta + \beta\gamma) + b\gamma\delta,$$
$$b' = a\beta^2 + 2d\beta\delta + b\delta^2, \quad c' = c.$$

Thus, binary form (a, d, b) of determinant $-C$ is transformed by substitution $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ into form (a', d', b') and we choose the substitution in such a way that a' is the least in absolute value of numbers representable by form (a, d, b) (for variables not simultaneously zero).

For this we must, for $-C < 0$ and for $-C > 0$ but not a square, transform (a, d, b) into a reduced form, and for $-C$ equal to a square (in particular, zero), transform (a, d, b) into form (a', d', b') with $a' = 0$. Remembering inequalities for the coefficients of reduced forms (§§ 3–5), we may write for all the cases $|a'| \leqq \sqrt{\frac{4}{3}|C|}$. Thus, a given ternary form can always be transformed by the substitution into a form whose first coefficient is connected with the third diagonal coefficient of the adjoined form by inequality $|a'| \leqq \sqrt{\frac{4}{3}|C'|}$.

This is Gauss's *first reduction*. Let us transform a given form f by substitution $\begin{pmatrix} 1 & 0 & 0 \\ 0 & \alpha & \beta \\ 0 & \gamma & \delta \end{pmatrix}$, $\alpha\delta - \beta\gamma = \pm 1$; since the adjoint substitution is $\begin{pmatrix} \pm 1 & 0 & 0 \\ 0 & \delta & -\gamma \\ 0 & -\beta & \alpha \end{pmatrix}$, we find for the transformed forms

$$a' = a, \quad B' = B\delta^2 - 2G\delta\beta + C\beta^2, \quad G' = -B\gamma\delta + G(\alpha\delta + \beta\gamma) - C\alpha\beta,$$
$$C' = B\gamma^2 - 2G\gamma\alpha + C\alpha^2.$$

Consequently, form (C, G, B) of determinant $G^2 - BC = -\alpha\Delta$ (Δ is the determinant of f) is transformed by substitution $\begin{pmatrix} \alpha & -\beta \\ -\gamma & \delta \end{pmatrix}$ into form (C', G', B'). Choosing this substitution in such a way that C' is the smallest value of form (C, G, B), we have for f' inequality $|C'| \leqq \sqrt{\frac{4}{3}|a'\Delta|}$. This is the *second reduction*, applying to a given form f first the first reduction, then the second, then the first one again, etc. we obtain a sequence of forms $f, f', f'', f''', \ldots$ and it is easy to see that after a finite number of operations we arrive at a form $f^{(n)}$ in which neither $|a^{(n)}|$ nor $|C^{(n)}|$ cannot be diminished, and for which we, consequently, have simultaneously $|a^{(n)}| \leqq \sqrt{\frac{4}{3}|C^{(n)}|}$, $|C^{(n)}| \leqq \sqrt{\frac{4}{3}|a^{(n)}\Delta|}$. In fact, otherwise we would have a chain of inequalities $|a| > |a'| = |a''| > |a'''| = |a''''| > \ldots$ which, clearly, cannot continue indefinitely. Hence, every ternary form is equivalent to a form f_0 whose first coefficient is connected with the third coefficient of the adjoined form by inequalities $|a_0| \leqq \sqrt{\frac{4}{3}|\Delta|}$, $|C_0| \leqq \sqrt{\frac{4}{3}|a_0\Delta|}$ from these inequalities we have $|a_0| \leqq \frac{4}{3}\sqrt[3]{|\Delta|}$, $|C_0| \leqq \frac{4}{3}\sqrt[3]{\Delta^2}$.

Now, let us transform form f_0 by a substitution $S = \begin{pmatrix} 1 & \beta & \gamma \\ 0 & 1 & \gamma' \\ 0 & 0 & 1 \end{pmatrix}$

which does not alter either a_0 or C_0. The coefficients of transformed forms f_0', F_0' satisfy

$$\begin{gathered} d_0' = d_0 + a_0\beta, \quad G_0' = G_0 - C_0\gamma' \\ E_0' = E_0 - G_0\beta + C_0(\beta\gamma' - \gamma) = E_0 - C_0\gamma - C_0'\beta \end{gathered} \tag{44}$$

Let us note that the quantities a_0, C_0 in form f_0 are either both distinct from zero, or both equal to zero (otherwise we may still apply the first or the second reduction to f_0). In the first case, it follows from (44) that with a suitable choice of integers β, γ', γ we have $|d_0'| \leqq \frac{1}{2}|a_0|$, $|G_0'| \leqq \frac{1}{2}|C_0|$, $|E_0'| \leqq \frac{1}{2}|C_0|$. In the second case, i.e. for $a_0 = C_0 = 0$, we have also $d_0 = 0$, $\Delta = -b_0 e_0$ (consequently b_0 and $e_0 \neq 0$); the formulae

$$g_0' = g_0 + b_0\gamma' + e_0\beta, \quad c_0' = c_0 + 2g_0\gamma' + b_0\gamma'^2 + 2e_0\gamma$$

show that in this case we may first choose β and γ' in such a way that $|g_0'|$ does not exceed half the greatest common divisor of b_0, e_0 (thus, $g_0' = 0$ for $(b_0, e_0) = 1$) and then choose γ in such a way that $|c_0| \leqq |e_0|$. Finally we find that every ternary form of determinant Δ is equivalent either to the form for which

$$\begin{gathered} 0 < |a| \leqq \tfrac{4}{3}\sqrt[3]{|\Delta|}, \quad 0 < |C| \leqq \tfrac{4}{3}\sqrt[3]{\Delta^2} \\ |d| \leqq \tfrac{1}{2}|a|, \quad |G| \leqq \tfrac{1}{2}|C|, \quad |E| \leqq \tfrac{1}{2}|C| \end{gathered} \tag{45}$$

or to the form for which

$$a = d = 0, \quad \Delta = -be^2, \quad |g| \leqq \tfrac{1}{2}(b, e), \quad |c| \leqq |e|.$$

Concerning the forms of the latter type, it is immediately clear, that their number is finite for a given $\Delta \neq 0$. In the forms of the first type (45) coefficients a, C, d and, consequently also $b = (d^2 + C)/a$ have a bounded number of values; from obvious relations

$$aE + dG + eC = 0, \quad dE + bG + gC = 0, \quad eE + gG + cC = \Delta,$$

we obtain

$$|e| \leqq \frac{|a| + |d|}{2}, \quad |g| \leqq \frac{|d| + |b|}{2}, \quad |c| \leqq \frac{|e| + |g|}{2} + |\Delta|,$$

consequently, the remaining coefficients e, g, c also have only a bounded number of values. Thus, theorem 17 is proved.

The Gaussian reduction is useful (especially for small Δ) also for practical computations. For example, performing it for $\Delta = \pm 1$, we obtain the following results. For $\Delta = +1$ ultimately two forms remain; $x^2+y^2+z^2$ and $-x^2+2yz$ which are not equivalent, since one is positive and the other is indefinite. Consequently, every positive ternary form of determinant $+1$ is equivalent to $x^2+y^2+z^2$ and every indefinite form is equivalent to $-x^2+2yz$. Similarly every positive ternary form of determinant -1 is equivalent to $-x^2-y^2-z^2$ and every indefinite form of determinant -1 is equivalent to x^2-2yz.

We say that an integer m, or a binary form $px^2+2qxy+ry^2$ is *representable* by a given ternary form $f(X, Y, Z)$ if there exist integers X_0, Y_0, Z_0 or linear forms

$$X = ax+a'y, \quad Y = bx+b'y, \quad Z = cx+c'y$$

for which $m = f(X_0, Y_0, Z_0)$ or $px^2+2qxy+ry^2 = f(X, Y, Z)$. The main problems of arithmetical theory of ternary forms were posed by Gauss in art. 278 "Disquisitiones Arithmeticae" [20] and is as follows: 1) find all representations of a given number by a given ternary form, 2) find all representations of a given binary form by a given ternary form, 3) investigate whether two given ternary forms are equivalent or not, and in the first case find all the substitutions transforming one form into another, 4) to find whether a given ternary form contains another ternary form, and, if so, find all substitutions transforming first form into the second. In the next section it will be shown that the solution of the first two questions in the case when the determinant of the ternary form is not equal to zero, is reduced to the solution of the third question. V. A. Markov (see [57])has shown that, in addition, the solution of the fourth question is reduced to the third. As far as the third question is concerned, we find, similarly to § 2, that its solution is composed of two parts: A) to find whether the two given ternary forms f, f' are equivalent or not and, in the first case to find *one* substitution transforming f into f'; B) find all integral substitutions of determinant ± 1, transforming the given form f into itself (the so called *automorphisms* of form f). On both these questions there is wide literature (papers by Seeber, Selling, Hermite and others), but the study of this literature is outside the limits of our monograph. Let us note one important particular case of question B): form $x^2+y^2+z^2$ is transformed into itself by means of 48 integral substi-

tutions of determinant ± 1, which are obtained by all possible permutations of variables x, y, z and their signs.

§ 14. Representations of numbers and binary forms by ternary forms

To find all representation of a given binary from $\varphi = pt^2 + 2qtu + ru^2$ by a given ternary form $f(x, y, z)$ we first consider the so called *proper* representations (Gauss [20] D. A. art. 280). Representation

$$pt^2 + 2qtu + ru^2 = f(\alpha t + \beta u,\ \alpha' t + \beta' u,\ \alpha'' t + \beta'' u) \qquad (46)$$

is called *proper* if determinants $\alpha'\beta'' + \alpha''\beta',\ \alpha''\beta - \alpha\beta'',\ \alpha\beta' - \alpha'\beta$ have no common divisor. Let (46) be any proper representation of φ by f; let us find three integers $\gamma, \gamma', \gamma''$ under the condition that the determinant of substitution $S = \begin{pmatrix} \alpha & \beta & \gamma \\ \alpha' & \beta' & \gamma' \\ \alpha'' & \beta'' & \gamma'' \end{pmatrix}$ is equal to $\varepsilon = \pm 1$, and let us transform f by this transformation into an equivalent form g. From (46) it is clear that the coefficients of x^2, xy and y^2 are, respectively, p, $2q$ and r so that matrix of g is of the form $\begin{pmatrix} p & q & m \\ q & r & n \\ m & n & s \end{pmatrix}$ (m, n, s are integers). Let d and Δ be determinants of forms φ and f (both not equal to zero). The substitution $\bar{S}$ adjoint to S transforms form F adjoint to f into form G adjoint to g. Noting that the elements of the third column of $\bar{S}$ are $\alpha'\beta'' - \alpha''\beta',\ \alpha''\beta - \alpha\beta'',\ \alpha\beta' - \alpha'\beta$ and that the third diagonal element in G is equal to $-d$ we obtain, by (43)

$$-d = F(\alpha'\beta'' - \alpha''\beta',\ \alpha''\beta - \alpha\beta'',\ \alpha\beta' - \alpha'\beta) \qquad (47)$$

Thus, *to every representation* (46) *of a binary form* φ *by a ternary form* f *there corresponds a representation* (47) *of number* $-d$ (*where* d *is the determinant of* φ) *by a form* F *adjoint to* f. It may be easily verified that this important proposition holds also for improper representations

Denoting by $\begin{pmatrix} P & Q & M \\ Q & R & N \\ M & N & -d \end{pmatrix}$ the matrix of form G we have

$$N^2 + Rd = -\Delta p,\quad MN + Qd = \Delta q,\quad M^2 + Pd = -\Delta r \qquad (48)$$

from which

$$-\Delta p \equiv N^2,\quad \Delta q \equiv MN,\quad -\Delta r \equiv M^2 \pmod{d} \qquad (49)$$

Therefore, $-\Delta$ must be *characteristic* number (§ 12) of the form (p_1-q, r) opposite to φ. Take instead of γ, γ', γ'' other integers $\delta, \delta', \delta''$ for which the determinant of substitution $S_1 = \begin{pmatrix} \alpha & \beta & \delta \\ \alpha' & \beta' & \delta' \\ \alpha'' & \beta'' & \delta'' \end{pmatrix}$ is equal to $\varepsilon_1 = \pm 1$, and let us see how this affects numbers M, N satisfying congruences (49). Let S_1 transform f into g_1 and let G_1 be the form adjoint with g_1. It is easy to see that substitution $T = S^{-1}S_1$ is of the form $\begin{pmatrix} 1 & 0 & \xi \\ 0 & 1 & \eta \\ 0 & 0 & \varepsilon\varepsilon_1 \end{pmatrix}$ where ξ, η are integers. Since substitution T transforms g into g_1, the adjoint substitution

$$T = \begin{pmatrix} \varepsilon\varepsilon_1 & 0 & 0 \\ 0 & \varepsilon\varepsilon_1 & 0 \\ -\xi & -\eta & 1 \end{pmatrix}$$

transforms G into G_1. From this we find the following expressions for new numbers M_1, N_1 corresponding to substitution S_1

$$M_1 = \varepsilon\varepsilon_1 M + d\xi, \quad N_1 = \varepsilon\varepsilon_1 N + d\eta.$$

so that $M_1 \equiv \varepsilon\varepsilon_1 M$, $N_1 \equiv \varepsilon\varepsilon_1 N \pmod{d}$. Thus, for an arbitrary change of the third column in the substitution S_1 (only its determinant must remain equal to ± 1), numbers M_1, N_1 remain congruent either with M, N or with $-M$, $-N$ modulo d. We shall say that a proper representation (46) of φ through f *belongs* to solution $\pm M$, $\pm N$ of system of congruences (49). Note, conversely, that ξ, η and $\varepsilon = \pm 1$ completely determine the substitution $S_1 = ST$ whose first two columns are α, α', α'' and β, β', β''. Consequently, by a suitable change of the third column of S we may transform M, N into *any* pair of numbers congruent to $\pm M$, $\pm N$ modulo d. From this we deduce the following method for finding all proper representations of a binary form φ through form f.

I. We find all solutions of system of congruences (49), not connected by conditions $M_1 \equiv \pm M$, $N_1 \equiv \pm N \pmod{d}$. For the case $(\Delta, d) = 1$ this problem was solved in § 12, where we saw that for (49) to be solvable in this case, it is necessary that φ is a primitive form.

II. Let M, N be one of the solutions of system (49). Defining integers P, Q, R from (48) we thus obtain the adjoint form G. Its

coefficients determine the coefficients m, n, s of form g either from equalities

$$dm = pM+qN, \quad dn = qM+rN, \quad ds = mM+nN-\Delta \tag{50}$$

or from

$$\Delta m = QN-MR, \quad \Delta n = QM-PN, \quad \Delta s = PR-Q^2 \tag{51}$$

If the obtained numbers m, n, s are not integers, then there are no proper representations of φ belonging to the given solution M, N of congruences (49). Note, that for $(\Delta, d) = 1$ the numbers m, n, s are *always* integers, which is evident from (50) and (51). Equalities (50) show that the determinant of the obtained integral form g is equal to Δ.

III. We investigate whether the constructed integral ternary form g of determinant Δ is equivalent to the given form (question 3 of the previous section). If g and f are not equivalent, then there exist no proper representations of φ belonging to solution M, N. If, however f and g are equivalent, then, taking two first columns α, α', α'', β, β', β'' from every substitution $S = \begin{pmatrix} \alpha & \beta & \gamma \\ \alpha' & \beta' & \gamma' \\ \alpha'' & \beta'' & \gamma'' \end{pmatrix}$ which transforms f into g, we obtain all proper representations of φ by f belonging to the given root M, N of system (49). Applying the same procedure to other solutions of system (49) we obtain, all proper representations of φ by f.

The following few remarks should be added to the above method.

1) The number of solutions of system (49), which are not connected by conditions $M_1 \equiv \pm M$, $N_1 \equiv \pm N \pmod{d}$ is, in general equal to half the number of solutions in a general sense (i.e. incongruent modulo d), apart from the case when there exist solutions M, N for which $M \equiv -M$, $N \equiv -N$, i.e. $2M \equiv 0$, $2N \equiv 0 \pmod{d}$. In the case $(\Delta, d) = 1$ which is of most interest to us, this may occur only for $d = \pm 1, \pm 2$; in fact, from (49) for $2M$, $2N$ divisible by d, it follows that $2\Delta p$, $2\Delta q$, $2\Delta r$ and consequently $2p$, $2q$, $2r$ are divisible by d, and since in this case p, q, r have no common factor (see I), we have $2 \equiv 0 \pmod{d}$, q.e.d.

2) In counting the number of representations of φ by f, two representations (46) and

$$pt^2+2qtu+ru^2 = f(\alpha_1 t+\beta_1 u, \alpha_1' t+\beta_1' u, \alpha_1'' t+\beta_1'' u)$$

are considered the same if and only if $\alpha = \alpha_1, \alpha' = \alpha_1', \ldots, \beta'' = \beta_1''$. It is clear from the reasoning above that two representations belonging to two distinct solutions of (49) (i.e. not connected by congruences $M_1 \equiv \pm M$, $N_1 \equiv \pm N$) are always distinct. Suppose now that two distinct substitutions S and S_1 transforming f into the same form g, give the same representation of φ by f, i.e. differ from each other only in their third column. Then substitution $T = S^{-1}S_1 = \begin{pmatrix} 1 & 0 & \xi \\ 0 & 1 & \eta \\ 0 & 0 & \varepsilon\varepsilon_1 \end{pmatrix}$ (ξ, η are integers, ε, ε_1 are determinants of S, S_1) transforms into itself, and T transforms g into itself. Therefore

$$\varepsilon\varepsilon_1 M+d\xi = M, \quad \varepsilon\varepsilon_1 N+d\eta = N,$$

thus, if $2M$, $2N$ are not simultaneously divisible by d then $\varepsilon_1 = \varepsilon$, $\xi = 0$, $\eta = 0$, $S_1 = S$. Thus, for $(\Delta, d) = 1$ and $|d| > 2$ distinct substitutions transforming f into g lead to different proper representations of φ by f.

3) Since forms f and g are equivalent, they are either both positive, or both negative, or both indefinite. Applying to g the conditions of positiveness and negativeness for a form given in § 13, we can say: if $\Delta > 0$ and f is positive, then for the existence of representations of φ by f the form φ must be positive (which is obvious also directly) if $\Delta > 0$ and f is indefinite, then either $d > 0$ or $d < 0, p < 0$ (i.e. φ is negative). Similarly, for $\Delta < 0$ and a negative f the form φ is negative; for $\Delta < 0$ and an indefinite f the form φ must be either indefinite, or positive.

To determine the *improper* representations of a binary form φ through f there exists the following method of Gauss (D.A. [20], art. 284). If representation (46) is improper, then the numbers $\alpha'\beta''-\alpha''\beta'$, $\alpha''\beta-\alpha\beta''$, $\alpha\beta'-\alpha'\beta$ have the greatest common divisor $e > 1$ and from (47) it is clear that e^2 divides d; we shall say that representation (48) *belongs* to number e. Denoting by $x > 0$ the greatest common divisor of numbers α, α', α'' and taking $\alpha = xa$, $\alpha' = xa'$ $\alpha'' = xa''$, $e = x\mu$ (μ - a positive integer) we find that determinants

$\alpha'\beta''-\alpha''\beta'$, $\alpha''\beta-\alpha\beta''$, $\alpha\beta'-\alpha'\beta$ are divisible by μ; from which (since a, a', a'' have no common factor) we deduce (§ 10, lemma I) that $\beta \equiv \lambda a$, $\beta' \equiv \lambda a'$, $\beta'' \equiv \lambda a''$ (mod μ), where λ is an integer, which may be assumed to be greater or equal to zero and less than μ. Taking $\beta = \lambda a+\mu b$, $\beta' = \lambda a'+\mu b'$, $\beta'' = \lambda a''+\mu b''$ we find that the determinants of matrix $\begin{pmatrix} \alpha & \alpha' & \alpha'' \\ \beta & \beta' & \beta'' \end{pmatrix}$ are equal to the corresponding determinants of matrix $\begin{pmatrix} a & a' & a'' \\ b & b' & b'' \end{pmatrix}$ multiplied by e, since the determinants of the latter matrix are numbers without a common factor. Introducing into (46) values

$$\begin{array}{lll} \alpha = \varkappa a, & \alpha' + \varkappa a' & \alpha'' = \varkappa a'', \\ \beta = \lambda a+\mu b, & \beta' = \lambda a'+\mu b', & \beta'' = \lambda a''+\mu b'' \end{array} \tag{52}$$

and taking $T = nt+\lambda u$, $U = \mu u$ we find

$$pt^2+2qtu+ru^2 = f(aT+bU, a'T+b'U, a''T+b''U).$$

In the right hand side is an integral binary form in variables. Thus, the substitution $t = (1/\varkappa)T-(\lambda/e)U$, $u = (1/\mu)\,U$ transforms φ into an integral form in variables T, U and expressions $aT+bU$, $a'T+b'U$, $a''T+b''U$ give a proper representation of this new form in terms of f. Thus, to obtain all representations of φ through f, which belong to a given square divisor e of d, we must proceed as follows: split e in all possible ways into a product of two integral positive factors n and μ and for every such decomposition give λ the values 0, 1, 2, . . ., $\mu-1$ and transform form φ by substitutions $\begin{pmatrix} 1/\varkappa & -\lambda/e \\ 0 & 1/\mu \end{pmatrix}$ of determinant $1/e$ into form φ', rejecting all those substitutions for which φ' is not an integral form. For every remaining substitution we find all proper representations a, a', a'', b, b', b'' of form φ' through f and by them we define the required representations α, α', α''; β, β', β'' by formulae (52). It is easy to see that in this way we obtain all representations of φ belonging to number e, and every representation occurs just once. Thus, determination of all representations of a binary form is reduced to the solution of the problem of equivalence of ternary forms (§ 13).

Before we consider the representation of numbers by ternary forms, we prove the following lemmas: (Gauss [20], D.A. art. 234, 279):

LEMMA I. *For every three integers a, a', a'' we can find a matrix of six numbers* $\begin{pmatrix} m & m' & m'' \\ n & n' & n'' \end{pmatrix}$ *for which* $m'n''-m''n' = a$, $m''n-mn'' = a'$, $mn'-m'n = a''$. Clearly, we may assume that a, a', a'' have no common factor. Take two non-proportional solutions p, p', p'' and n, n', n'' of equation $ax+a'x'+a''x'' = 0$ (if, for example $a \neq 0$, then we may take $p = a'$, $p' = -a$, $p'' = 0$ and $n = a''$, $n' = 0$, $n'' = -a$); then $p'n''-p''n' = \mu a$, $p''n-pn'' = \mu a'$, $pn'-p'n = \mu a''$ where $\mu \neq 0$ is an integer. If $\mu \neq \pm 1$, then assuming (that n, n', n'' have no common factor) by lemma I § 10 we may write $p \equiv \lambda n$, $p' \equiv \lambda n'$, $p'' \equiv \lambda n''$ (mod μ). Taking $p = \lambda n+\mu m$, $p' = \lambda n'+\mu m'$, $p'' = \lambda n''+\mu m''$ we obtain numbers m, m', m''; n, n', n'' which possess the required property.

LEMMA II. *If two rectangular matrices* $\sigma = \begin{pmatrix} m & n \\ m' & n' \\ m'' & n'' \end{pmatrix}$ *and* $\tau = \begin{pmatrix} g & h \\ g' & h' \\ g'' & h'' \end{pmatrix}$ *have the same determinants, i.e.*

$$m'n''-m''n' = g'h''-g''h' = L,$$
$$m''n-mn'' = g''h-gh'' = L', \quad mn'-m'n = gh'-g'h = L'',$$

where L, L', L'' have no common factor, then there exists an integral square matrix $S = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ *of determinant $+1$, for which $\tau = \sigma S$ (in the multiplication the rows of σ are multiplied by columns of S).* From the conditions of the lemma we see that we may select integers l, l', l'' such that the determinants of matrices $A = \begin{pmatrix} m & n & l \\ m' & n' & l' \\ m'' & n'' & l'' \end{pmatrix}$ and $B = \begin{pmatrix} g & h & l \\ g' & h' & l' \\ g'' & h'' & l'' \end{pmatrix}$ are equal to $+1$, therefore $A^{-1}B$ is an integral matrix of the form $\begin{pmatrix} \alpha & \beta & 0 \\ \gamma & \delta & 0 \\ 0 & 0 & 1 \end{pmatrix}$; matrix $S = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ has determinant $+1$ and possesses the required property.

Gauss's method for determining the representations of a given number by a given ternary form (D.A. [20], art. 280) is based on formula (47) and is closely connected with the problem of the representation of a binary form, which has already been considered

here. The representations of a number is, as usually, called *proper* if the representing numbers have no common factor. Clearly, it suffices to find all the proper representations of a given number. Let $d \neq 0$ be the determinant of binary forms, let f be a given ternary form, let F be a form united with it. Formula (47) shows that to every proper representation (46) of any binary form $\varphi = pt^2+2qtu+ru^2$ of determinant d through f there corresponds a proper representation

$$-d = F(a, a', a''), \quad a = \alpha'\beta''-\alpha''\beta', \quad a' = \alpha''\beta-\alpha\beta'', \quad a'' = \alpha\beta'-\alpha'\beta$$

of number $-d$ by an adjoint form F; we shall say that representation a, a', a'' of number $-d$ by F *belongs* to representation α, α', α'', β, β', β'' of form φ through f. Concerning the belonging, the following conclusions may be drawn:

1) Every proper representation a, a', a'' of number $-d$ through F belongs to a proper representation of a form φ of determinant d through f. In fact, let us determine (Lemma I) the six numbers α, α', α'', β, β', β'' in such a way that the cofactors of the third column of matrix $S = \begin{pmatrix} \alpha & \beta & 0 \\ \alpha' & \beta' & 0 \\ \alpha'' & \beta'' & 0 \end{pmatrix}$ are equal to a, a', a'', and consider a binary form of variables t, u

$$\varphi = f(\alpha t+\beta u, \quad \alpha' t+\beta' u, \quad \alpha'' t+\beta'' u).$$

This form is a result of transformation of f by substitution S. If we consider φ as a ternary form and construct a form adjoint to it, then its third diagonal coefficient is $-d'$ where d' is the determinant of φ; on the other hand, noting that the elements of the third column in $\bar{S}$ are a, a', a'' and, taking into account equality $F(a, a', a'') = -d$, we obtain $d' = d$. Thus, representation a, a', a'' belongs to the proper representation α, α', α'', β, β', β'' of form φ of determinant d through f.

2) Let binary form φ be equivalent to form ψ and let it transform into it by means of substitution $S = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ of determinant $+1$. Then to every proper representation of φ through f

$$\varphi = f(mt+nu, m't+n'u, m''t+n''u) \tag{53}$$

corresponds a proper representation of ψ

$$\psi = f(gt'+hu', g't'+h'u', g''t'+h''u') \tag{54}$$

where $t = \alpha t'+\beta u'$, $u = \gamma t'+\delta u'$ and

$$\begin{aligned} g &= m\alpha+n\gamma, & h &= m\beta+n\delta; \\ g' &= m'\alpha+n'\gamma, & h' &= m'\beta+n'\delta; \\ g'' &= m''\alpha+n''\gamma, & h'' &= m''\beta+n''\delta. \end{aligned} \tag{55}$$

Writing (53) and (54) as matrices $\sigma = \begin{pmatrix} m & n \\ m' & n' \\ m'' & n'' \end{pmatrix}$ and $\tau = \begin{pmatrix} g & h \\ g' & h' \\ g'' & h'' \end{pmatrix}$ we may write the relation (55) as equality $\tau = \sigma S$, with usual definition of matrix multiplication. It follows from (55) that

$$\begin{aligned} m'n''-m''n' &= g'h''-g''h' \\ m''n-mn'' &= g''h-gh'' \\ mn'-m'n &= gh'-g'h \end{aligned} \tag{56}$$

i.e. to representations of φ and ψ by b, denoted by matrices σ and τ, belongs the same proper representation of $-d$ by F. Thus, representation of every form ψ equivalent to φ by form f, yields the same representation of $-d$ by F, as do the representations of φ. This result holds also in the case $\varphi = \psi$, i.e. when δ is a substitution transforming φ into itself.

3) Conversely, if two representations (53) and (54) of forms φ and ψ of determinant d through f lead to the same proper representation of $-d$ by F, i.e. if (56) holds, then by lemma II there exists an integral matrix $S = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ of determinant $+1$ for which $\tau = \sigma S$. In other words, the given representations are connected by relation (55). Therefore, by (53) and (54) φ transforms into ψ by substitution S. It is clear from the above reasoning how to proceed in order to find all proper representations of $-d$ by form F. Let $\varphi_1, \varphi_2, \ldots$ be all non-equivalent binary forms of determinant d, which allow proper representations by f. Let us find for every form φ_i all its proper representations by f, whose matrices $\sigma_i', \sigma_i', \sigma_i'', \ldots$ are not connected by relations $\sigma_i^{(k)} = \sigma_i^{(l)}S$, where S in the substitution transforming φ_i into itself. Passing from the obtained representations by f to representations of $-d$ by F, we obtain by (47) all proper representations of $-d$ by form F and every one occurs just once.

A general case, when it is required to represent any number $M \neq 0$ by a given ternary form f of determinant $\Delta \neq 0$ is easily reduced to the particular case considered above. If F is the form adjoint with f, then Δf is adjoint with F. Since our problem is equivalent to finding all representations of ΔM by forms Δf, to solve it we must consider proper representations of binary forms of determinant $-\Delta M$ by a ternary form F. Thus, the problem of finding the representations of a number by a given ternary form is also reduced to the third problem of Gauss (§ 13).

§ 15. Application of Rédei theorem to binary forms

The methods described above allow us directly to prove Gauss's theorem on genera (§ 12, theorem 16). Let $F = (A, B, C)$ be a given form of the principal genus of determinant d (so that F is properly primitive and for $d < 0$ a positive form). We shall look for proper representations of the opposite form $F' = (A, -B, C)$ by a ternary form $f = x^2 - 2yz$. It is not difficult to see that all conditions necessary for the existence of proper representations (§ 14) are satisfied in the given case. In fact, (cf. I, II, III, § 14): I. Since determinant of f is $\Delta = -1$ and F belongs to the principal genus, it follows that $-\Delta = 1$ is a characteristic number of F (§ 12) so that the system of congruences (49) has solution M, N. II. Constructing for every solution M, N a ternary form g (see § 14, formulae (51)), we find that g is an integral form of determinant -1. III. The constructed form is an indefinite form (since F is positive for $d < 0$), and since by § 13 every indefinite form of determinant -1 is equivalent to f, then forms f and g are equivalent.

Taking substitution $S = \begin{pmatrix} \alpha & \beta & \gamma \\ \alpha' & \beta' & \gamma' \\ \alpha'' & \beta'' & \gamma'' \end{pmatrix}$ of determinant ± 1 transforming f into g, we find the required representation of F' by f

$$Ax^2 - 2Bxy + Cy^2 = (\alpha x + \beta y)^2 - 2(\alpha' x + \beta' y)(\alpha'' x + \beta'' y). \quad (57)$$

Denoting numbers $\alpha\beta' - \alpha'\beta$, $\alpha'\beta'' - \alpha''\beta'$, $\alpha''\beta - \alpha\beta''$ by a, b, c we obtain from (57) and (47)

$$A = \alpha^2 - 2\alpha'\alpha'', \quad B = -\alpha\beta + \alpha'\beta'' + \alpha''\beta', \quad C = \beta^2 - 2\beta'\beta''$$
$$d = b^2 - 2ac. \quad (58)$$

Numbers a, b, c have no common factor; it is easy to show that at least one of the numbers a, c is odd, so that of two forms $\varphi = (2a, -b, c)$, $\psi = (a, -b, 2c)$ (determinant of which by (58) is equal to d) one is properly primitive. In fact, for a and c even, b is odd and equalities $b\alpha+c\alpha'+a\alpha'' = 0$, $b\beta+c\beta'+a\beta'' = 0$ show that α and β are even, form which by (58) we conclude that A, C are even, which is impossible since F is a properly primitive form. From (58) we deduce that the substitution

$$X = 2\beta' xx' + \beta xy' + \beta yx' + \beta'' yy',$$
$$Y = 2\alpha' xx' + \alpha xy' + \alpha yx' + \alpha'' yy'$$

transforms (in Gauss's terminology § 10) form $F(X, Y)$ into product $\varphi(x, y)\varphi(x', y')$; similarly, the substitution

$$\begin{aligned} X &= \beta' xx' + \beta xy' + \beta yx' + 2\beta'' yy' \\ Y &= \alpha' xx' + \alpha xy' + \alpha yx' + 2\alpha'' yy' \end{aligned} \tag{59}$$

transforms F into product $\psi\psi$. It follows from § 10, that to check these statements it suffices to verify the system of relations (29). It was noted above that one of the forms φ, ψ (ψ, say) is properly primitive. Thus, from transformability of F into $\psi\psi$ and from the fact that F and ψ have the same determinant d, and by Gaussian properties of the composition (§ 10, conclusion 3), we see that F is *compounded* from ψ and ψ (which may be proved directly by verifying that six determinants of substitution (59) have no common divisor). Thus, the class of form F is the square of the class of ψ, which, by § 12, proves the theorem on genera. The present proof of theorem 16 is based on Gaussian composition. The same theorem may be proved by means of a more simple Dirichlet composition (§ 10), if we use formula (57). We have seen above that one of numbers $a = \alpha\beta' - \alpha'\beta$, $c = \alpha''\beta - \alpha\beta''$ is odd; taking a to be odd, we prove that numbers α, α', α''; β, β', β'' may be so chosen that a is relatively prime to $2d$. In fact, substitution $T = \begin{pmatrix} 1 & 0 & 2r \\ 2r & 1 & 2r^2 \\ 0 & 0 & 1 \end{pmatrix}$ (r is an integer) transforms $f = x^2 - 2yz$ into itself; replacing thus the above substitution S, transforming f into g, by the substitution $TS = \begin{pmatrix} \alpha_1 & \beta_1 & \gamma_1 \\ \alpha_1' & \beta_1' & \gamma_1' \\ \alpha_1'' & \beta_1'' & \gamma_1'' \end{pmatrix}$ we find that the numbers

$\alpha_1, \alpha_1', \alpha_1'', \beta_1, \beta_1', \beta_1''$ also give a proper representation of form F' by f. Evaluating for these numbers the value $a_1 = \alpha_1\beta_1' - \alpha_1'\beta_1$ we obtain $a_1 = a + 2cr^2 - 2br$ i.e. a quadratic polynomial in r, whose coefficients have no common factor, and whose value, for a suitable choice of r, is relatively prime to $2d$. Thus, in representation (57) of form F' by f we may assume the number $a = \alpha\beta' - \alpha'\beta$ to be relatively prime to $2d$. Taking in (57) $x = \beta'$, $y = -\alpha'$ we obtain $F(\beta', \alpha') = a^2$, i.e. the given form F represents a perfect square, relatively prime to $2d$. Therefore, F is equivalent to a form (m^2, l, n) where m is relatively prime to $2d$; moreover, from $l^2 - m^2n = d$ it is clear, that m is relatively prime to $2l$ too, i.e. that the form $(m, l, mn) = \varphi$ is concordant to itself (§ 10). Determinant of φ is equal to d. Compounding φ with φ by Dirichlet (§ 10), we, clearly, obtain the form (m^2, l, n). Thus, class of F is the square of the class of φ in the sense of the Dirichlet's composition. Q.e.d.

Recently (1933) Rédei [73] has observed an interesting theorem which complements Gauss's classical result on the number of invariants of the group of classes, equal to powers of 2 (§ 10). Consider the group of properly primitive classes of forms of determinant d, positive for $d < 0$. Rédei's theorem determines the number of invariants of this group, which are of the form 2^α, $\alpha \geqq 2$, i.e. which are divisible by 4 (see Rédei [73]).

Denoting by n the number of these invariants, and by m the number of invariants equal to 2^1 (so that the total number of invariants equal to powers of 2 is $m+n$), it is easy to see that the numbers of classes K for which $K^4 = 1$, is equal to $2^m 4^n = 2^{m+n}2^n$. Assuming $K^2 = A$, we find $A^2 = 1$, i.e. A is an ambiguous class belonging to the principal genus. Conversely, if A is an ambiguous class belonging to the principal genus, then, taking $A = K^2$ by the theorem 16 proved in this section, we obtain $K^4 = 1$. Two classes K and K' for which $K' = KA_0$ (A_0 is an ambiguous class) correspond to the same class A, and the number of ambiguous classes is 2^{m+n}. Hence, we may say that the number of distinct ambiguous classes belonging to the principal genus is 2^n. Assuming $d \equiv 1 \pmod 4$ we remember that in this case all ambiguous classes are obtained by means of the forms $(a, 0, a')$ (§ 9), where $-d = aa'$ and a and a' are relatively prime (for $d < 0$, $a > 0$ and $a' > 0$). Thus, to every decomposition of number d into two relatively prime factors $-d = cc'$ there exists an ambiguous class,

determined by form $(c, 0, c')$. Factorisation $-d = cc'$ will be called the *product* of two factorisations $-d = aa'$ and $-d = bb'$ if the class of $(c, 0, c')$ is the product of classes of $(a, 0, a')$ and $(b, 0, b')$. Several factorisations $-d = aa'$, $-d = bb'$, ... will be called independent if the ambiguous classes A, B, ... corresponding to them are not connected by a relation of the form $A^x B^y \ldots = 1$ where at least one index x, y, ... is odd. Let us now note that ambiguous classes belonging to the principal genus form a group whose basis consists of n independent elements. On the other hand, form $(a, 0, a')$ belongs to the principal genus if and only if $(a/p') = 1$ for every prime p' of a' and $(a'/p) = 1$ for every prime p of a (i.e. every one of numbers a, a' is a quadratic residue of the other). Combining these remarks, we may formulate Rédei's theorem: *In a group of classes. The number of invariants, which are divisible by* 4 *is equal to the number of independent factorisations of* $-d$ *into two relatively prime factors* a, a' *each of which is the quadratic residue of the other.* A similar result is obtained in the case $d \not\equiv 1 \pmod 4$. Reichardt [74] generalised this last theorem to the case of invariants divisible by any power of 2.

§ 16. The representation of numbers and binary forms by three squares

We apply the general theory of the representation of a number and of a binary form by a ternary form f (§ 14) to a particular case $f = x^2+y^2+z^2$. Consider first the proper representations of a given binary form $\varphi = (p, q, r)$. For such representations to exist φ must be positive, primitive, and have -1 as a generic number. Denoting the determinant of φ by $-n$ and remembering the result of § 12, we may say that either $n \equiv 1, 2 \pmod 4$ (and φ is properly primitive), or $n \equiv 3 \pmod 8$ (and then φ is improperly primitive). In both cases φ must belong to a completely determined genus G_0 for which the values of the generic characters are of the form $(-1/p)$, $(-1/p')$, ... Under those conditions, system (49) § 14 has $2^{(n)}$ solutions (§ 12); Moreover, a ternary form g constructed by the rule II (§ 14) is always an integral form, equivalent to $x^2+y^2+z^2$ (§ 13). Assuming $n > 2$ and taking into account the fact that form $x^2+y^2+z^2$ has 48 automorphisms (§ 13) we may say be remarks 1 and 4 of § 14, that φ has $48 \cdot 2^{(n)-1} = 24 \cdot 2^{(n)}$ proper representations by $x^2+y^2+z^2$. This result, as it is easy to see, (Gauss [20] D.A. art. 290), is true also for the

omitted cases $n = 1, 2$. Therefore: *In order that there exist proper representations of a given positive binary form φ of determinant $-n$ as a sum of three squares, it is necessary and sufficient that either $n \equiv 1, 2 \pmod 4$ and then φ belongs to genus G_0 of a properly primitive order, or $n \equiv 3 \pmod 8$ and then φ belongs to genus G_0 of an improperly primitive order. In both cases G_0 is determined by the values of characters $\chi_i(\varphi) = (-1/p_i)$ (p_i are all odd prime divisors of n). Under these conditions the number of representations of φ as a sum of three squares is* $24 \cdot 2^{(n)}$. From this, by the method of § 14, it is easy to deduce the number of proper representations of a given number n as a sum of three squares. Since the form $x^2+y^2+z^2$ coincides with its adjoint form, the question is reduced to considering the proper representations of binary forms of determinant $-n$ by $x^2+y^2+z^2$. Consequently, for proper representations to exist, we must have $n \equiv 1, 2 \pmod 4$ or $n \equiv 3 \pmod 8$ (which can be seen also directly, from equation $n = x^2+y^2+z^2$ when x, y, z have no common factor.). Let $\varphi_1, \varphi_2, \ldots$ be all non-equivalent forms of genus G_0 of determinant $-n$; assuming n distinct from 1 and 3 we may say that every form φ_i transforms into itself only by substitutions $\begin{pmatrix} \pm 1 & 0 \\ 0 & \pm 1 \end{pmatrix}$. Therefore, by the rule of § 14, we must omit half of $24 \cdot 2^{(n)}$ proper representations of φ_i by $x^2+y^2+z^2$. Noting, finally, that the number of forms φ_i is equal to $h/2^{(n)}$ for $n \equiv 1, 2 \pmod 4$ and to $h'/(2^{(n)-1})$ for $n = 3 \pmod 8$ (h, h' are numbers of properly and improperly primitive classes) we obtain the following theorem of Gauss (D. A. [20], art. 291).

THEOREM 18. *The number of representations of a given number $n > 0$ as a sum of three coprime squares, is equal to $12h$ for $n \equiv 1, 2 \pmod 4$ and $24h'$ for $n \equiv 3 \pmod 8$ where h and h' are the numbers of properly and improperly primitive classes of positive forms of determinant $-n$, and the number n is assumed distinct from 1 and 3.*

For $n = 1$ and $n = 3$ the numbers of proper representations by form $x^2+y^2+z^2$ are 6 and 8 respectively, so that for these cases theorem is not true. Fermat has already noticed (only in a different form) the *possibility* of representing a number of the form $8m+3$ by a sum of three squares (The so called Fermat theorem on figurate numbers, see notes to the present chapter). The precise number of these representations for the case of a prime n was found by induction by

Legendre (see [39], p. 388); but neither Fermat nor Legendre gave the strict proof of their statements, and it was first done by Gauss. Another proof of theorem 18, based on Liouville's methods will be given in chapter VI. We must note that up until now there is no concize elementary proof (i.e. independent of the theory of quadratic forms) even of the *possibility* of the representation of a given number of form $4n+1$, $4n+2$, or $8n+3$ as a sum of three squares[1] (see notes to the present chapter, p. 271).

Theorem 18 enables us to find the number of *all* representations $N_3(n)$ of a given number $n > 0$ as a sum of three squares (and, as usually, two representations $n = x^2+y^2+z^2$, $n = x'^2+y'^2+z'^2$ are considered the same only if $x = x'$, $y = y'$, $z = z'$). To obtain a final expression for $N_3(n)$ we introduce two new integral functions $F(n)$ and $G(n)$ as follows. Let $\overline{G(n)}$ be the number of *all* classes of positive binary forms of determinant $-n$; $\bar{F}(n)$ denotes the number of classes of forms with odd divisor (i.e. the forms which have at least one odd end coefficient). Assume, for every $n > 0$

$$F(n) = \bar{F}(n) - \underset{n=s^2,\, s \text{ odd}}{\left\{\tfrac{1}{2}\right\}}, \quad G(n) = \bar{G}(n) - \underset{n=s^2}{\left\{\tfrac{1}{2}\right\}} - \underset{n=3s^2}{\left\{\tfrac{2}{3}\right\}}, \tag{60}$$

where the symbol $\left\{\frac{1}{2}\right\}_{n=s^2,\, s \text{ odd}}$ denotes $\frac{1}{2}$ when n is equal to an odd square, and 0 otherwise; other symbols have a similar meaning. Functions $F(n)$, $G(n)$ occur frequently in chapter VI. Denoting by $h(m)$ the number of properly primitive positive classes of forms of determinant $-m$, we may write for every n

$$\bar{F}(n) = \sum h\left(\frac{n}{\delta^2}\right), \tag{61}$$

where the summation is performed over odd square divisors δ of number n. Now, let us note a few important relations existing between functions $N_3(n)$, $F(n)$, $G(n)$, which follow from theorems 14, 15 and 18. For $n \equiv 1, 2 \pmod 4$ every form of determinant $-n$ has

---

[1] An elementary proof of the representability of a number as a sum of three squares performed by using Liouville's identitities (+) and (7), ch. VI, p. 322 and similar ones, may be found in Uspensky's *Theory of Numbers* (1939), p. 455.

More recent results are: L. J. Mordell On the representation of a number as a sum of three squares. Revue de mathématiques pures et appliquées. Tome III, 1958. No 1, 25–57. Ankeny Sums of three squares. Proc. Amer. Math. Soc. 1957 (8) 316–319.

at least one end coefficient odd, and consequently $\bar{G}(n) = \bar{F}(n)$. Taking into account formulae (60), (61) and theorem 18, we find

$$N_3(n) = 12F(n), \quad G(n) = F(n) \qquad \text{for } n \equiv 1, 2 \pmod 4 \tag{62}$$

For $n \equiv 3 \pmod 4$ we have

$$\bar{G}(n) = \sum h\left(\frac{n}{\delta^2}\right) + \sum h'\left(\frac{n}{\delta^2}\right), \tag{63}$$

where both sums are taken over all square divisors of n, and $h'(m)$ denotes the number of improperly primitive positive classes of determinant $-m$. First, let $n \equiv 7 \pmod 8$; then n clearly, cannot be represented as a sum of three squares. Moreover, by theorem 14, we have $h'(n/\delta^2) = h(n/\delta^2)$ so that finally

$$N_3(n) = 0, \quad G(n) = 2F(n) \qquad \text{for } n \equiv 7 \pmod 8 \tag{64}$$

Similarly, from theorems 14, 18 and from (60), (61), (63), we obtain

$$N_3(n) = 8F(n) \quad G(n) = \tfrac{4}{3}F(n) \qquad \text{for } n \equiv 3 \pmod 8 \tag{65}$$

Finally, let n be divisible by 4, i.e. $n = 4m$. It follows from equation $4m = x^2+y^2+z^2$ that all numbers x, y, z are even, so that $N_3(4m) = N_3(m)$; applying, further, theorem 15, we obtain for every m

$$N_3(4m) = N_3(m), \quad F(4m) = 2F(m), \quad G(4m) = G(m)+2F(m) \tag{66}$$

Collecting all the cases considered above, we obtain the following theorem: *The number $N_3(n)$ of representations of n by a sum of three squares is expressed for every $n > 0$ as follows*:

$$N_3(n) = 12[2F(n)-G(n)], \tag{67}$$

where functions $F(n)$ and $G(n)$ are defined by (60).

Consider the number of all representations of a given binary form

$$kx^2+2lxy+k'y^2 \tag{68}$$

as a sum of three squares, and let us restrict ourselves to the case when the first coefficient k is *square free*. Under this assumption, the greatest common divisor of k, l and k' may be represented in the form PQ where P is the product of those primes p which enter into $kk'-l^2$

with an even power α; and Q is the product of primes q entering into $kk'-l^2$ with an odd power β. Further, denote by N the product of primes n which divide k and l but do not divide k'. In the case when there are no primes of a type p, q, n, the corresponding number P, Q or N is assumed to be one. Take

$$k = PQNR, \quad kk'-l^2 = \prod p^{\alpha} \prod q^{\beta} NL. \tag{69}$$

Numbers P, Q, N, R, L are all positive and, as it may be easily seen, they are coprime. Now, we can formulate the following theorem (B. A. Venkov [96]): *For a form* (68) *to be representable as a sum of squares of three integral linear forms in variables* x, y,

$$(ax+a'y)^2+(bx+b'y)^2+(cx+c'y)^2 \tag{70}$$

the following conditions are necessary and sufficient: 1) $-QNL$ *is a quadratic residue of* P *and* $-PRL$ *is a quadratic residue of* QN, 2) *every odd prime factor* r *of* L, *for which* $(-k/r) = -1$, *enters into* L *with an even power. Under these conditions the number* S *of representations of form* (68) *by* (70) *is equal to*

$$S = 24 \cdot 2^{(PQN)} \sum \left(\frac{-k}{\partial}\right) \tag{71}$$

where (PQN), *as always, denotes the number of distinct prime divisors of* PQN, *and the summation is performed over all odd divisors* ∂ *of* U.

The proof of this theorem is based on Gauss's method for the determination of improper representations of form (68) by $x^2+y^2+z^2$, described in § 14. According to this method, in order to obtain all representations of (68), belonging to a given square divisor e of number $kk'-l^2$, in the form (70), the form (68) must be transformed by substitutions of the form

$$T = \begin{pmatrix} \frac{1}{\varkappa} & -\frac{\lambda}{e} \\ 0 & \frac{1}{\mu} \end{pmatrix} (\varkappa > 0,\ \mu > 0,\ e = \varkappa\mu,\ \lambda = 0, 1, \ldots, \mu-1)$$

into a form $\varphi = (A, B, C)$ of determinant $-D = (l^2-kk')/e^2$, after which we keep those substitutions T, for which form φ is an integral form, representable by $x^2+y^2+z^2$. If the number of such substitutions is denoted by g, the number of all representations of form (68),

belonging to divisor e is equal to $24 \cdot 2^{(D)}g$ by the theorem at the beginning of the present section. The required number S of all representations is expressed as a sum $24 \sum 2^{(D)}g$ taken over all square divisors e of number $kk'-l^2$. Since, by assumption, k is square free, it follows that for the first coefficient of $\varphi = (A, B, C)$ to be an integer it is necessary that $x = 1$, $\mu = e$, $\lambda = 0, 1, \ldots, c-1$. Then the coefficients of φ are:

$$A = k, \quad B = \frac{l-k\lambda}{e}, \quad C = \frac{k'-2l+k\lambda^2}{e^2} \tag{72}$$

If form φ is an integral form, then in order that it has representations as a sum of three squares, it must satisfy the following conditions (theorem at the beginning of the present section): 1) it must be primitive 2) the number $D = AC-B^2 = (kk'-l^2)/e^2$ must be $\equiv 1, 2 \pmod 4$ or $\equiv 3 \pmod 8$ in the latter case φ must be improperly primitive, 3) for every odd prime r from D, $(-C/r) = 1$ if r divides A, and $(-A/r) = 1$ if r does not divide A. To simplify these conditions, we note that condition 2, provided that conditions 1 and 3 are satisfied, may be replaced by the following: $D \not\equiv 0 \pmod 4$. In fact, when D is not divisible by 4, either $D \equiv 1, 2 \pmod 4$ or $D \equiv 3 \pmod 4$; in the latter case form φ cannot be properly primitive, since otherwise the product of the characters $\chi(\varphi)$ corresponding to primes r, entering into D with odd power, would be equal to -1 by condition 3), which contradicts the relationship between the generic characters in a properly primitive order. (see (36), § 12). Thus, for $D \equiv 3 \pmod 4$, φ must be an improperly primitive form; applying to it relations between generic characters in improperly primitive order (see (37) § 12) we obtain, by condition 3, $-1 = (2/D)$, from which $D \equiv 3 \pmod 8$. Thus, condition 2 follows from $D \not\equiv 0 \pmod 4$.

Therefore, the values e, λ must be so selected that coefficients of form φ, defined by (72), satisfy the following conditions: a) numbers A, B, C are integers, b) A, B, C have no common factor, c) $D = AC-B^2 \not\equiv 0 \pmod 4$ d) for every odd prime r from D we have; either $(-A/r) = 1$, for $A \not\equiv 0$, or $(-C/r) = 1$ if $A \equiv 0 \pmod r$. It is evident from (72) that if φ satisfies conditions a) and b), then every prime factor u, common to k, l, k' divides e and in such a way that D is not divisible by u^2 (the latter follows from $D = AC-B^2$); conversely, if e contains every prime factor u, common to k, l, k'

and if $D = (kk' - l^2)/e^2$ is not divisible by u^2, then the form φ, *if it has integer coefficients*, is primitive. Remembering the definition of numbers $P, Q \ldots, L$ see((69)), we may assume $e_1 = \prod p^{\frac{1}{2}\alpha} \prod q^{\frac{1}{2}(\beta-1)}$ where e_1 is a squared factor of L, so that $L = e_1^2 L_1$ and $G = (kk' - l^2)/e^2 = Q, NL_1$. Since QN is not divisible by a square, and is relatively prime to L, the condition c) for form φ, i.e. $D \not\equiv 0 \pmod 4$, is equivalent to the following: $L_1 \equiv 0 \pmod 4$. Further, condition d) for φ splits into two: d') $-k$ is a quadratic residue of L_1, (which is equivalent to condition 2 formulated in the theorem) and d'') $-C$ is a quadratic residue of QN. Rewriting $D = AC - B^2$ in the form $L_1 = PRC - QN(B/QN)^2$ we see that condition d'') is equivalent to the following: $-PRL$ is a quadratic residue of QN (see condition 1 of the theorem). Clearly, all these conditions (written under the assumption that φ is an integral form) do not impose any restriction on λ in formulae (72): thus, we select λ in such a way that B and C are integers. Since $(k, e) = PQ$ and since PQ divides l, it follows that all λ for which B is an integer, are of the form $\lambda = \lambda_0 + (e/PQ)v$, where λ_0 is the least of such λ, and $v = 0, 1, 2, \ldots, PQ-1$. Taking $B_0 = (l - k\lambda_0)/e$ and noting that e is relatively prime to NR, we find that coefficient C is an integer together with the number

$$NR\,\frac{k' - 2l\lambda + k\lambda^2}{e^2} = \frac{(B_0 - NRv)^2 + D}{PQ}. \tag{73}$$

Since $D = QNL_1$ is divisible by Q, we have $B_0 - NRv \equiv 0 \pmod Q$, which defines the residue of v modulo Q. Further, for (73) to be an integer, it is necessary that either $-D$ or $-QNL$ is a quadratic residue of P (see condition 1 of the theorem). Under this condition there exists $g = 2^{(P)}$ values of v modulo P for which (73) is an integer and the same number of substitutions T (for a given e) for which φ is an integral form and satisfies all the above conditions. The total number of representations of form (68) as a sum of three squares is expressed as follows:

$$S = 24 \sum 2^{(D)} g = 24 \cdot 2^{(PQN)} \sum 2^{(L_1)},$$

where the last sum is taken over all representations of L in form $L = e_1^2 L_1$ $(e_1 > 0)$ for which L_1 is not divisible by 4, and $-k$ is a quadratic residue of L_1. This sum may now be easily represented as expression (71).

The theorem just proved has an important application in chapter VI in the proof of so-called Dirichlet formulae.

Notes to chapter 4

§ **1.** Systematic exposition of Gaussian theory of quadratic forms, apart from Gauss's [20] "Disquisitiones Arithmeticae" and standard textbooks on the theory of numbers mentioned in the notes to § 1, ch. I, see also the litographed lectures notes by Bianchi "Lezioni sulla teoria aritmetica delle forme quadratiche binarie e ternarie" [5] (1911–1912). In Russian, this theory, (together with relevant analytic results of Dirichlet) is described in litographic lectures by Grave called "Arithmetical theory of algebraic quantities" (1910). Other bibliographic references may be found in vol. III of Dickson's "History of the theory of numbers". An integral function $f(n)$, expressing the number of representations of a given number n by a binary form (of a positive or negative determinant) is studied by G. Pall [67, 68].

§ **4.** Minima $\sqrt{\frac{4}{5}d}$ and $\sqrt{\frac{1}{2}d}$ found in this section for forms $\sqrt{\frac{4}{5}d}(x^2+xy-y^2)$ and $\sqrt{\frac{1}{2}d}(x^2+2xy-y^2)$ present only the first terms of an infinite series of such minima given by A. A. Markov in his dissertation "On binary quadratic forms of a positive determinant" [54]. Denote by

$$\sqrt{n_1 d}, \quad \sqrt{n_2 d}, \quad \sqrt{n_3 d}, \ldots \tag{74}$$

the minima, and by

$$f_1, \quad f_2, \quad f_3 \tag{75}$$

the corresponding indefinite binary forms of determinant $d > 0$. The first terms of these series are as follows

$$n_1 = \tfrac{4}{5}, \quad n_2 = \tfrac{1}{2}, \quad n_3 = \tfrac{100}{221}, \ldots; \quad f_1 = \sqrt{\tfrac{4}{5}d}(x^2+xy-y^2),$$
$$f_2 = \sqrt{\tfrac{1}{2}d}(x^2+2xy-y^2), \quad f_3 = \sqrt{\tfrac{4}{221}d}(5x^2+11xy-5y^2), \ldots$$

A. A. Markov proves that series (74) and (75) have the following properties: 1) numbers $n_1, n_2, n_3, \ldots$ are strictly decreasing and tend to limit $\frac{4}{9}$; for every k, $\sqrt{n_k d}$ is a minimum of the form f_k for integer values of variables, not simultaneously zero.

2) If an indefinite binary form f of determinant d cannot be made less in absolute value than $\sqrt{n_k d}$ by means of integer values of its

variables, not simultaneously zero, then it is equivalent to one of the forms $f_1, f_2, \ldots, f_k$ and, consequently, its minimum is one of the numbers $\sqrt{n_1 d}, \sqrt{n_2 d}, \ldots, \sqrt{n_k d}$.

3) Every number n_k is of the form $1/(\frac{9}{4} - 1/p^2)$ where $p > 0$ is an integer which has the following property: we may select an infinite number of pairs of integers $q > 0$, $r > 0$ which are connected with p by equation $p^2 + q^2 + r^2 = 3pqr$. Conversely, for every solution of this indeterminate equation, in positive integers p, q, r the numbers $1/(\frac{9}{4} - 1/p^2)$, $1/(\frac{9}{4} - 1/q^2)$, $1/(\frac{9}{4} - 1/r^2)$ are contained in the series $n_1, n_2, \ldots$. Moreover, A. A. Markov gives a simple method for determining all solutions of equation $p^2 + q^2 + r^2 = 3pqr$. The above results are obtained in the study of certain periodic continued fractions, closely connected with Johann Bernoulli's problem (see § 13, ch. II).

Another simple proof of the main theorem of this section (if two reduced forms of a positive determinant are equivalent, then one of them is contained in the period of the other) was given by Mertens [58], it is restricted to the case of integral forms.

§§ 1–12. The exposition on quadratic forms here follows Gauss's classical notation in which the binary form is written as $(a, b, c) = ax^2 + 2bxy + cy^2$ (with *even* middle coefficient). However, in some parts of the modern theory of numbers (for example, in the theory of ideals), it is more appropriate to write the form as $\{a, b, c\} = ax^2 + bxy + cy^2$ with any (even or odd) coefficient b. The determinant of form $\{a, b, c\}$ is $d = b^2 - 4ac$ so that determinant d is always either of form $4k$, if b is even, or of the form $4k+1$ if b is odd. Form $\{a, b, c\}$ is *primitive*, if numbers a, b, c have no common factor. Transition from Gauss's notation to notation $\{a, b, c\}$ is performed by means of the following obvious propositions: 1) if b is even, the primitive form $\{a, b, c,\}$ is, in fact a *properly primitive* form $(a, \frac{1}{2}b, c)$ of determinant $\frac{1}{4}d$ in Gauss's notation, 2) for odd b, $\{a, b, c\} = \frac{1}{2}(2a, b, 2c)$ where $(2a, b, 2c)$ is *improperly primitive* form of determinant $d \equiv 1 \pmod 4$ in Gauss's notation. For the reader's convenience, we given here formulation of the main statements in notation $\{a, b, c\}$.

Transformation. If a form $\{a, b, c\}$ is transformed into $\{a', b', c'\}$ by substitution $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$, then the coefficients of the new form are expressed as

$$a' = a\alpha^2+b\alpha\gamma+c\gamma^2, \quad b' = 2a\alpha\beta+b(\alpha\delta+\beta\gamma)+2c\gamma\delta,$$
$$c' = a\beta^2+b\beta\delta+c\delta^2.$$

Conditions for a form to be reducible. For $d < 0$: $|b| \leqq a \leqq c$ for $d > 0$ and not a square, $0 < \sqrt{d}-b < |2a| < \sqrt{d}+b$.

Dirichlet composition. Two forms $\{a, b, c\}$ and $\{a', b', c'\}$ of the same determinant are *concordant* if numbers a, a', $\frac{1}{2}(b+b')$ have no common factor (the number $\frac{1}{2}(b+b')$ is, clearly, always an integer).

Ambiguous classes. Let determinant $d = b^2-4ac$ be not equal to a square, then for $d \equiv 1 \pmod 4$ the number of ambiguous classes is $2^{(d)-1}$ and for $d \equiv 0 \pmod 4$ it is equal to the number of ambiguous classes for Gaussian determinant (see end of § 9).

Generic characters. Let n be a number representable by a primitive form $\{a, b, c\}$ and let n and $2d$ be relatively prime. Then the generic characters of $\{a, b, c\}$ for $d \equiv 1 \pmod 4$ are (n/p), (n/p'), ... where $p, p' \ldots$ are all distinct prime factors of d. For $d \equiv 0 \pmod 4$ generic characters of $\{a, b. c\}$ coincide with the generic characters of the properly primitive order of Gaussian determinant $\frac{1}{4}d$ (§ 12). The number of genera (for d not a square) is always equal to the number of ambiguous classes.

§ 13. A complete exposition on the theory of ternary forms is given in L. Bianchi's [5] book, mentioned above in the note to § 1, and also in Bachmann's book 'Die Arithmetik des quadratischen Formen' [3]. In Russian, the exposition on *positive* ternary forms may be found in V. A. Markov's dissertation 'On positive ternary quadratic forms' [57] (1897).

§ 14. The problem of the representation of *zero* by means of the given indefinite ternary form is reduced to the solution in integers of an indefinite equation $ax^2+by^2+cz^2 = 0$ (Gauss [20], D.A. art. 299). In considering this equation we may restrict ourselves to the case when integers a, b, c are coprime and are not divisible by a square (Gauss D.A. art. 298). Under this assumption, the conditions of solubility, and the solutions of equation $ax^2+by^2+cz^2 = 0$ may be found either from general theorems on ternary forms (§ 14), (see Gauss [20], D.A. art. 294–295), or by means of another more elementary method of of Dedekind (see L. Dirichlet [14], § 156). In this case we obtain the following theorem:

Let a, b, c be integers, not equal to zero, coprime and not divisible by a square. Equation $ax^2+by^2+cz^2 = 0$ *has solutions if and only if*: 1) *a, b, c are not all of the same sign*; 2) *numbers* $-bc$, $-ca$, $-ab$ *are quadratic residues to moduli a, b, c respectively. Let these conditions be satisfied and let* α, β, γ *be any numbers satisfying congruences* $\alpha^2 \equiv -bc \pmod{a}$, $\beta^2 \equiv -ca \pmod{b}$, $\gamma^2 \equiv -ab \pmod{c}$, *then equation* $ax^2+by^2+cz^2 = 0$ *has an infinite number of proper solutions* (i.e. *such solutions for which ax, by, cz have no common factor*), *satisfying the following conditions* $\alpha z \equiv by \pmod{a}$, $\beta x \equiv cz \pmod{b}$, $\gamma y \equiv ax \pmod{c}$.

Concerning the representations of numbers by means of a complete system of positive ternary forms of a given determinant see Albert A. Adrian (1933) 'On the representation by indefinite ternary forms', see also Ross [75] (1933).

§ 15. Another proof of Gauss's theorem on genera, based on the solution of equation $ax^2+by^2+cz^2 = 0$. (see the previous note) is given by Dedekind (L. Dirichlet [14], § 157).

§ 16. Theorems on decomposition of numbers and binary forms into a sum of three squares (§ 16, ch. IV and § 2, ch. VI) may be proved also by means of the arithmetic of quaternions (see B. A. Venkov [95]). Gauss's theorem 18 is connected with a theorem of Fermat on so-called figurate numbers, i.e. numbers of the form $(q-2)\frac{1}{2}(n(n-1)) + n$ $(q = 3, 3, 5, \ldots, n = a, \pm 1, \pm 2, \ldots)$. for $q = 3$, we obtain *triangular* numbers $\frac{1}{2}(n(n+1))$, for $q = 4$ they are *square* numbers, for $q = 5$ – *pentagonal* numbers etc. Their name originated from a simple geometrical construction which had been used by ancient mathematicians, in which these numbers are distributed at the vertices of a regular triangle, quadrangle, etc. In particular, pentagonal numbers play an important part in the partitioning of a number (see ch. V) Fermat stated without proof the following theorem:

Every natural number is a sum of no more than three triangular, numbers, no more than four square numbers, no more than five pentagonal numbers, etc. It is easy to deduce from theorem 18 the proof of this statement for triangular and square numbers. In fact, by theorem 18 the number $8n+3$ $(n > 0)$ is a sum of three squares, which, clearly, must be odd; therefore, we may write $8n+3 = (2x+1)^2+(2y+1)^2 + (2z+1)^2$, which gives $n = \frac{1}{2}x(x+1)+\frac{1}{2}y(y+1)+\frac{1}{2}z(z+1)$. Concerning the sum of four squares, we find that numbers $n \equiv 1, 2$

(mod 4) and $n \equiv 3 \pmod 8$ are sums of three squares (by theorem 18) in the case $n \equiv 7 \pmod 8$ the number $n-1$ is twice an odd number, and thus $n-1 = x^2+y^2+z^2$, $n = x^2+y^2+z^2+1^2$. Therefore, every number not divisible by 4 (and therefore, every integer) is a sum of four squares. In general, Fermat's theorem was proved by Cauchy in 1815 (see Bachmann [3], p. 154).

5. PARTITIONS. LIOUVILLE'S METHODS

§ 1. Point graphs. The Euler-Legendre theorem

Classical theory of numbers given in the previous chapters is mainly based on the composition of integers from prime factors by means of multiplication and thus it may be called a multiplicative theory of numbers. In the present chapter we shall be concerned with another part of the theory of numbers which has been studied much less, namely – the additive theory of numbers. In fact, it would be premature to call this domain of study a 'theory', since it lacks the general methods and general viewpoints which characterise every theory; its state reminds us greatly of the state of number theory before the appearance of the 'Disquisitiones Arithmeticae' by Gauss.

The beginning of this part of the theory of numbers has originated from the famous studies of Euler in his memoires 'De partitione numerorum' (see [17], vol. I, p. 73) and known under the name of theorems on partitions (partitio numerorum). Euler obtained his theorems analytically, deducing various relations between power series, and equating the coefficients of equal powers of the variable. The present section gives arithmetical proofs of the most important theorems of Euler.

Denoting by x and z the variables whose moduli are less than one, and expanding of the infinite products $\prod_{n=1}^{\infty}(1+x^n)$ and $\prod_{n=1}^{\infty}(1+x^n z)$ into power series of x and z, assume

$$\begin{aligned} \prod_{n=1}^{\infty}(1+x^n) &= 1+\sum_{n=1}^{\infty}\lambda(n)x^n, \\ \prod_{n=1}^{\infty}(1+x^n z) &= 1+\sum_{n,\,m-1}^{\infty}\lambda(n,\,m)x^n z^m \end{aligned} \tag{1}$$

Clearly, $\lambda(n)$ is the number of partitions[1] of n into any number of

[1] Partition of a number n is a representation of n as a sum of any number of integral parts. H.A.

unequal integral non-negative parts. In counting the partitions, we assume two partitions to be the same if they differ only in order of their terms. For 6 we have the following partitions: $1+2+3=1+5=2+4=0+6$, $\lambda(6)=4$. Similarly, the symbol $\lambda(n, m)$ denotes the number of partitions of n into m unequal integral positive parts. Further, from

$$\prod_{n=1}^{\infty}\frac{1}{1-x^n}=1+\sum_{n=1}^{\infty}\bar{\mu}(n)x^n,\quad \prod_{n=1}^{\infty}\frac{1}{1-x^nz}=1+\sum_{n,m=1}^{\infty}\mu(n,m)x^nz^m, \quad (2)$$

$$\prod_{n=1}^{\infty}(1+x^{2n-1})=1+\sum_{n=1}^{\infty}\nu(n)x^n,\quad \prod_{n=1}^{\infty}\frac{1}{1-x^{2n-1}}=1+\sum_{n=1}^{\infty}\rho(n)x^n \quad (3)$$

we obtain the following integral functions: $\bar{\mu}(n)$ is the number of partitions of n into any number of positive integral parts some of which may repeat (e.g. for 6 we have $1+1+1+1+1+1=1+1+1+1+2=1+1+1+3=1+1+2+2=1+1+4=1+2+3=2+2+2=1+5=2+4=3+3=6$; $\bar{\mu}(6)=11$. In our notation $\bar{\mu}(n)$, the bar on the top is used to distinguish it from the Möbius function $\mu(n)$ (see § 2, ch. I). $\mu(n, m)$ is the number of partitions of n into m parts as in the previous case, $\nu(n)$ is the number of partitions of n into unequal positive odd parts, and $\rho(n)$ is the number of partitions of n into positive odd parts, some of which may repeat. All these quantities (so called arithmetical functions) have many remarkable properties, which are described in the present and the following section. Denoting the left hand side of the second formula (2) by $f(z)$, Euler obtained for this function the relation $f(xz)=(1-xz)f(z)$ from which he deduces

$$1+\sum_{n,m=1}^{\infty}\mu(n,m)x^nz^m=1+\sum_{m=1}^{\infty}\frac{x^m}{(1-x)(1-x^2)\dots(1-x^m)}z^m.$$

Comparison of the coefficients of $x^nz^m (n>m)$ in both sides of this equality gives the following theorem:

1) *The number of partitions of $n>m$ into m parts is equal to the number of partitions of $n-m$ into parts the largest of which is m.*

Symbolically, this theorem may be written as

$$N(n=x_1+x_2+\dots+x_m,\ 0<x_1\leqq x_2\leqq\dots\leqq x_m,\ x_i-\text{integers})$$
$$=N(m-n=1\xi_1+2\xi_2+\dots+m\xi_m,\ \xi_i-\text{integers}\geqq 0) \quad (4)$$

where N denotes the number of partitions, characterised in brackets

after letter *N*. Similarly, we obtain the following theorem (in formulation of this and the following theorems of the present section a 'part' will mean an 'integral positive part'):

2) *The number of partitions of* $n(n > \frac{1}{2}(m(m+1))$ *into* m *unequal parts is equal to the number of partitions of* $n-\frac{1}{2}(m(m+1))$ *into any number of parts, some of which may be equal.*

Further, on proving the identity

$$\prod_{n=1}^{\infty}(1+x^n) = \prod_{n=1}^{\infty}\frac{1}{1-x^{2n-1}},$$

Euler obtains $\lambda(n) = \rho(n)$ for every n, or:

3) *The number of partitions of* n *into unequal parts is equal to the number of its partitions into odd parts.*

Another important theorem, though not formulated by Euler, clearly follows from his formula below. Intending to prove a recurrence relation for the sum of divisors, which he discovered (see below, theorem 20) in 'Demonstratio theorematis circa ordinem in summis divisiorum observati', Euler proves the relationship

$$\prod_{n=1}^{\infty}(1-x^n) = \sum_{k=-\infty}^{+\infty}(-1)^k x^{\frac{1}{2}(3k^2-k)}, \tag{5}$$

which presents one of the most used formulae of the present theory of the elliptic functions. The exponents on the right hand side of (5) are *pentagonal* numbers $\omega_k = \frac{1}{2}(3k^2-k)$ (see notes to ch. IV). Their values for the first few numbers are $\omega_0 = 0$, $\omega_1 = 1$, $\omega_{-1} = 2$, $\omega_2 = 5$, $\omega_2 = 7$, $\omega_3 = 12$, $\omega_{-3} = 15$ etc. Comparing the coefficients of x^n on both sides of (5) we obtain the following theorem which is called the Euler-Legendre theorem:

THEOREM 19. *The difference between the number of partitions of* n *into even parts, and the number of partitions of* n *into odd parts, is equal to zero if* n *is not a pentagonal number, and to* $(-1)^k$ *if* n *is a pentagonal number* ω_k.

The method used for an arithmetical proof of the above theorems is the method of point graphs, used by English authors of the Sylvester school. Let a partition of a number be given as follows: $n = x_1+x_2+\ldots+x_m$, $0 < x_m \leqq x_{m-1} \leqq \ldots \leqq x_1$; We represent this partition graphically by an array of dots on the plane, situated along m rows, the dots in a row corresponding to a part. The first row

contains x_1 dots, the second x_2 dots, etc., . . . the m-th row has x_m dots. The first dots of rows are situated in the first column, and the distances between neighbouring dots along horizontal and vertical lines are the same. A system of points distributed in such a way will be called the *graph* corresponding to the partition. For example, the left graph of fig. 1 is the graph of partition of 13 into $5+3+3+2$. Clearly, every column of a graph is not longer that the column preceeding it. Moreover, if the graph represents a partition of a number into unequal parts, the number of dots in two neighbouring columns are either equal, or they differ by one.

Let us prove now theorem 1) by means of graphs. Taking a graph of an arbitrary partition of n into m parts, some of which may be the same, we note that the first column of the graph contains m dots, and every subsequent column – not more than m dots. We omit the first column, and interchange rows and columns in the remaining graph

Fig. 1

(the first row into first column, the second row into the second column, etc.). Clearly, we obtain a partition of number $n-m$ into parts some of which may be equal, none of the parts exceeding m. Conversely, taking any graph of a partition of $n-m$ into parts not exceeding m, some of which may repeat, interchange rows and columns and write on the left a column of m dots, we obtain the graph of a partition of n into m parts, equal or not. On the left in fig. 1 is the partition of $n = 13$ into $m = 4$ parts $5+3+3+2$ and on the right – the corresponding partition of $n-m = 9$ into parts $4+3+1+1$, not exceeding 4. Thus, partitions on the right and on the left hand sides of (4) are brought into one-to-one correspondence and, consequently, the number of these partitions are the same, q.e.d. Theorem 2) can be proved similarly.

Theorem 3) may also be proved by means of graphs, but the following proof is even simpler. It is known from elementary arithmetic that every integer is uniquely representable in a system to the base p (p is an integer > 1), i.e. in the form $a_0+a_1p+a_2p^2+\ldots+a_kp^k$ where the 'digits' $a_0, a_1, \ldots a_k$ have values out of the set 0, 1, 2, . . ., $p-1$. For $p = 2$ we find that every number may be represented uniquely as a sum of several distinct powers of 2. Now, let

$$n = v_1+v_1+\ldots+v_2+v_2+\ldots \tag{6}$$

be any partition of n into odd parts some of which may be the same, where $v_1, v_2, \ldots$ denote distinct odd numbers and each v_i enters partition (6) m_i times, so that $n = m_1v_1+m_2v_2+\ldots$. Representing, thus, every number m_i in the form $2^{a_{i1}}+2^{a_{i2}}+\ldots$ we obtain

$$n = 2^{a_{11}}v_1+2^{a_{12}}v_1+\ldots+2^{a_{21}}v_2+2^{a_{22}}v_2+\ldots$$

i.e. partition of n into even or odd parts

$$2^{a_{11}}v_1, 2^{a_{12}}v_1, \ldots, 2^{a_{21}}v_2, 2^{a_{22}}v_2, \ldots$$

which, clearly, are distinct. Conversely, if we have a partition $n = k_1+k_2+\ldots$ into distinct parts k_i we represent each part in the form $k_i = 2^{a_i}v_i$ ($a_i \geqq 0$, v_i odd), and collect terms with the same v_i. Assuming the sum of $2^{a_i}v_i+2^{a'_i}v_i+\ldots$ of these terms equal to m_iv_i (where $m_i = 2^{a_i}+2^{a'_i}+\ldots$ we obtain $n = m_1v_1+m_2v_2+\ldots$ i.e. a partition of n into odd parts, where $v_1, v_2, \ldots$ are distinct and v_i enters into the partition m_i times. Thus, the number $\lambda(n)$ of partitions of n into unequal (odd or even) parts is equal to the number $\rho(n)$ of partitions of n into parts some of which may be equal, q.e.d.

We pass to the proof of theorem 19 of Euler-Legendre by the graph method. Take a graph representing a partition of n into unequal parts in descending order. Draw a line at 45° to the horizontal direction through the last dot of the first row of the graph (see fig. 2, on the left); this line is called the *slope* of the graph. Let l denote the number of dots of the graph lying on the slope, and let k denote the number of dots on the lowest line of the graph. All graphs, representing partitions of n into unequal parts, may be divided into two classes: the first class consists of the graphs in which $l > k$ the second class of those with $l < k$. We agree to call graphs *exceptional* if they are graphs of the first class which have $l = k$ and in which the last dot of

the lowest line is on the slope, and the graphs of the second class in which $l = k-1$ and the last dot of the lowest line is on the slope. Exceptional graphs of the first class correspond to the partitions of the form $k+(k+1)+\ldots+(2k-1) = \frac{1}{2}(3k^2-k) = \omega_k \quad (k > 0)$, the exceptional graphs of the second class belong to the partitions of the form $(l+1)+(l+2)+\ldots+2l = \frac{1}{2}(3l^2+l) = \omega_{-l}\,(l > 0)$. This makes it clear that if n is non-pentagonal, then there are no exceptional graphs. If $n = \omega_s$ then this equality completely determines the integer $s \gtrless 0$ and in this case there exists only one exceptional graph, belonging to the first class when $s = k > 0$ and to the second class when $s = -l < 0$, the number of rows of such a graph is equal to $|s|$. Let us prove that non-exceptional graphs of the first and second class may be brought into a one-to-one correspondence with each other. Take a non-exceptional graph and, omitting its last line, let us add its k dots to the first k rows. Then we obtain a graph whose slope contains k dots, and the last line has more than k dots. This graph is, consequently, of the second class and non-exceptional. In fact, if the slope of the obtained graph ends in its last line, this line contains no less than $k+2$ dots. Fig. 2 on the left has an exceptional graph of the first class ($k = 2, l = 3$), corresponding to partition of number $17 = 6+5+4+2$, and on the right it has the non-exceptional graph of second class obtained from it by the described method. Conversely, let us take a non-exceptional graph of second class and let us put l dots of its slope as a last row. Then we obtain a new graph whose slope contains at least l dots and whose last row contains l dots, which, consequently, is a graph of the first class and is a non-exceptional graph. In fact, if the slope of the new graph ends at its last row, then the slope line has at least $l+1$ dots. Thus, non-exceptional graphs of the first and second class are brought into a one-to-one correspondence; moreover, the numbers of rows of two corresponding graphs differ always by one. Therefore, if we consider only those partitions of n which correspond to non-exceptional graphs, then the number of partitions with an even number of parts is always equal to the number of partitions with odd number of parts. From here theorem 19 follows if we take into account the fact that for a non-pentagonal number n there are no exceptional graphs, and a pentagonal number $n = \omega_s$ has one exceptional graph, whose number of rows is of the same parity as s.

Fig. 2

Closely connected with the theorem of Euler-Legendre is the famous theorem of Euler on the number of divisors $\zeta(n)$ of n (§ 2, ch. I) (see Euler [17], p. 234):

THEOREM 20. *For every $n > 0$ we have*

$$\sum (-1)^k \zeta(n-\omega_k) = \{(-1)^{s-1} n\}_{n=\omega_s} \tag{7}$$

where the summation on the left hand side is performed over all numbers $k \gtreqless 0$ for which $\omega_k < n$, and symbol $\{(-1)^{s-1} n\}_{n=\omega_s}$ denotes 0 for n equal to non-pentagonal number, and $(-1)^{s-1} n$ when $n = \omega_s$.

Consider all possible representations of n in the form $n = \sum_m a + d\delta$ where $\sum_m a$ is a sum of m unequal parts of a, d and δ are positive numbers; sum $\sum_m a$ may be absent. We extend sum $S = \sum(-1)^m d$ over all representations above; evaluation of this sum in two ways gives formula (7).

Firstly, collecting in S all terms for which $d\delta = p$ has the same value, we find the totality of all such terms equal to $\zeta(p)\sum(-1)^m$ where $\sum(-1)^m$ is taken over all partitions of number $n-p$ into unequal parts. Applying theorem 19, we find for S expression $S = \sum_{\omega_k < n} (-1)^k \zeta(n-\omega_k)$. To find another expression for S, we split all representations $n = \sum_m a + d\delta$ into three categories: 1) representations in which d does not occur among the terms of the sum $\sum_m a$, and $\delta > 1$, 2) representations in which d occurs among the terms of sum $\sum_m a$, 3) representations in which d does not occur among terms of $\sum_m a$ and $\delta = 1$. Take a representation of the first category $n = \sum_m a + d\delta$ and, taking away one d from $d\delta$, we adjoin it as a term to the sum $\sum_m a$; the obtained representation which may be written as $n = \sum_{m+1} a + d(\delta - 1)$ belongs, clearly, to the second category. Conversely, from every representation of the second category we can

obtain, by means of a reverse process, a representation of the first category. Thus, representations of the first and second category are in a simple one-to-one correspondence. Noting that the terms of sum S for the corresponding representations, i.e. $(-1)^m d$ and $(-1)^{m+1} d$ cancel each other out, we may say that the part of the sum S extended over the representations of both categories is equal to zero. Consider now a representation of the third category $n = \sum_m a + d$; since d does not occur among the parts of a this representation may be considered as a partition of n into $m+1$ unequal parts Conversely, from every partition of n into $m+1$ parts $n = a_1 + a_2 + \ldots + a_{m+1}$ we obtain $m+1$ representations of the third category on making d equal, successively, to $a_1, a_2, \ldots, a_{m+1}$. These $m+1$ representations of the third category give in the sum S the terms $(-1)^m a_1 + (-1)^m a_2 + \ldots + (-1)^m a_{m+1} = (-1)^m n$ from which it is clear that the whole sum S is equal to $-n\sum(-1)^m$ where $\sum(-1)^m$ is taken over all possible partitions of n into m unequal parts, and by theorem 19 $S = \{(-1)^{s-1} n\}_{n=\omega_s}$. Comparing the two expressions for S we obtain formula (7).

Euler himself has proved formula (7) by logarithmic differentiation of the identity (5). Formula (7) enables us to evaluate the values of $\zeta(n)$ successively, without factorising n into prime factors.

§ 2. Double partitions. Recurrence relations for additive functions

Partitions of the form $n = \sum_m a + d\delta$ used in the previous section for the proof of theorem 20, are examples of double partitions in which every number is partitioned in all possible ways into a sum of two parts $n = u + v$, after which the numbers u, v are partitioned, independently of each other, by the method given above. In the present section we give further examples of dual partitions and apply them to deduce some recurrence relations similar to (7) for additive functions $\lambda(n)$, $\bar{\mu}(n)$, $\nu(n)$. Consider all possible partitions of $n > 0$ of the form $n = \sum_m a + \sum a^*$ where $\sum_m a$ denotes a partition into unequal parts a (m not fixed) and sum $\sum a^*$ denotes a partition where some parts may be the same. Each sum $\sum_m a$, $\sum a^*$ may be absent. Denote by $N((-1)^m;\ n = \sum_m a + \sum a^*)$ the sum $\sum(-1)^m$ over all described partitions and let us prove that *for every* $n > 0$ we have

$$N((-1)^m;\ n = \sum_m a + \sum a^*) = 0 \tag{8}$$

To prove this, collect into one group all those partitions $n = \sum_m a + \sum a^*$ in which the sets of parts of a and a^* are the same. Let this set contain k unequal terms. Clearly, all partitions of a group are obtained when we select from k given terms a set of m parts ($m = 0, 1, 2, \ldots, k$) and enter them into sum $\sum_m a$, whilst the remaining partitions will belong to $\sum a^*$. Thus, for $m = 0, 1, 2, \ldots, k$ we obtain $1, C_k^1, C_k^2, \ldots, C_k^k$ double partitions (C_k^l denotes the number of combinations of k elements taken l at a time), and the sum $\sum(-1)^m$ constructed for them is $1 - C_k^1 + C_k^2 - \ldots \pm C_k^k = 0$. Consequently, part of sum $\sum(-1)^m$ constructed for any group of partitions is already equal to zero, and therefore, the whole sum is equal to zero, so that (8) is proved.

Of theorems similar to (8) let us point out one which is proved similarly:

$$N((-1)^m; n = \sum_m a + \sum b) = N((-1)^m; n = 2\sum_m a). \tag{9}$$

In the left hand side the parts $\sum_m a$ and $\sum b$ are the sums of unequal parts, each of them may be absent. The remaining notations need no explanation.

Collecting in the sum in the left hand side of (8) the terms for which $\sum_m a = u$ and $\sum a^* = v$ have the same value ($u+v = n$) we find, by the Euler-Legendre theorem that this part of the sum is equal to zero if u is not a pentagonal number, and equal to $(-1)^k \bar{\mu}(v)$ if $u = \omega_k$; moreover, we assume $\bar{\mu}(0) = 1$. Thus, equality (8) gives the following value for function $\bar{\mu}(n)$: *for every* $n > 0$

$$\sum_{\omega_k \leqq n} (-1)^k \bar{\mu}(n - \omega_k) = 0 \tag{10}$$

where on the left hand side the summation is performed over all numbers $k \geqq 0$ *satisfying the condition written under the summation sign.* Formula (10) is very similar to the well known relation satisfied by the Möbius function $\mu(n)$, which was proved in § 2, ch. I, and yields the same results as it does there. Namely, we may prove the inversion formula similar to the classical inversion formula for $\mu(n)$ (§ 2, ch. I). Let $f(n)$ and $F(n)$ be two given numerical functions defined for all the values of $n \geqq 0$ connected by relation

$$\sum_{\omega_s \leqq n/h} (-1)^s f(n - h\omega_s) = F(n) \tag{11}$$

where $h > 0$ is a given integer. Then, conversely, for every $n \geqq 0$ we have

$$f(n) = \sum_{0 \leqq k \leqq n/h} \bar{\mu}(k) F(n-hk). \tag{12}$$

To prove this, we put into the right hand side of (12) the value of $F(n-hk)$ from (11)

$$F(n-hk) = \sum_{s} (-1)^s f(n-h(k+\omega_s));$$

then we obtain

$$\sum \bar{\mu}(k) F(n-hk) = \sum_{k,\, s} (-1)^s \bar{\mu}(k) f(n-h(k+\omega_s)).$$

Combining in the last sum the terms with equal value of $k+\omega_s = l$ we obtain

$$\sum_{0 \leqq l \leqq n/h} f(n-hl) \sum_{\omega_s \leqq l} (-1)^s \bar{\mu}(l-\omega_s).$$

By (10) the inner sum is reduced to zero for every $l > 0$, so that the above double sum is equal to $f(n)$, which proves formula (12). Applying the Euler-Legendre theorem to both sides of (9) we obtain a recurrence relation for function $\lambda(n)$ (taking $\lambda(0) = 1$):

$$\sum_{\omega_k \leqq n} (-1)^k \lambda(n-\omega_k) = \{(-1)^s\}_{n=2\omega_s}. \tag{13}$$

Using the inversion formula (12) we obtain from here an expression of $\lambda(n)$ through $\bar{\mu}(n)$:

$$\lambda(n) = \sum_{2\omega_k \leqq n} (-1)^k \bar{\mu}(n-2\omega_k). \tag{14}$$

In order to deduce a similar recurrence relation for function $\nu(n)$ (§ 1), we use the Euler-Legendre theorem, which in notation used at present, may be written as

$$N((-1)^m; n = \sum_{m} a) = \{(-1)^s\}_{n=\omega_s}.$$

Separating even terms $2b$ and odd terms i in sum $\sum_m a$, denoting their numbers by α and β respectively, and noting that $m \equiv \alpha+\beta \equiv \alpha+n \pmod 2$ we may write

$$N((-1)^\alpha; n = 2\sum_{\alpha} b + \sum_{\beta} i) = \{(-1)^{n+s}\}_{n=\omega_s}.$$

Applying the Legendre-Euler theorem again to the left hand side and remembering the last definition of function $v(n)$ we obtain

$$\sum_{2\omega_k \leqq n} (-1)^k v(n-2\omega_k) = \{(-1)^{n+s}\}_{n=\omega_s}. \tag{15}$$

From this, with help of (12), we may express $v(n)$ through $\bar{\mu}(n)$. Formulae (10), (13) and (15) allow us to evaluate, successively, the values of functions $\bar{\mu}(n)$, $\lambda(n)$ and $v(n)$ without using a real partition of numbers. (See notes to this chapter, p. 190).

In his dissertation Vahlen [83] has proved a theorem generalising the Euler-Legendre theorem. Considering the partitions n of into distinct parts, let us consider the least residue of each part modulo 3, i.e. a number $\varepsilon = 0, 1$ or -1 for which $a \equiv \varepsilon \pmod 3$. Then Vahlen's theorem may be formulated as follows: *if we consider only those partitions of n into distinct parts* $n = \sum_m a$ *for which the sum of least absolute residues modulo* 3 *is equal to a given number h, then the sum* $\sum(-1)^m$ *taken over all those partitions is equal to zero for* $n \neq \omega_h$ *and is equal to* $(-1)^h$ *for* $n = \omega_h$.

Without pausing to prove this theorem, let us note one of its corollaries:

$$N((-1)^{k+l+m};\ n = \sum_k a + \sum_l b + \sum_m c) = \{(-1)^{i-1}(2i-1)\}_{n=\frac{1}{2}(i^2-i),\ i>0}. \tag{16}$$

On the left hand side the sums $\sum_k a$, $\sum_l b$, $\sum_m c$ denote, as usual the sums of k, l and m distinct parts respectively; each of these sums may be absent. Applying the Euler-Legendre theorem to the left hand side of (16) we may present it in the form $N((-1)^{\alpha+\beta+\gamma};\ n = \omega_\alpha + \omega_\beta + \omega_\gamma)$. Noting that $24\omega_\alpha + 1 = (6\alpha-1)^2$ and taking $8n+1 = p$ we obtain from (16) the following *Jacobi theorem*: for every integer $p = 1 \pmod 8$ we have

$$\sum_{3p=(6\alpha-1)^2+(6\beta-1)^2+(6\gamma-1)^2} (-1)^{\alpha+\beta+\gamma} = \{(-1)^{\frac{1}{2}(s-1)}s\}_{p=s^2,\ s>0} \tag{17}$$

where on the left hand side the summation is performed over all representations of $3p$ *in the form given under the summation sign, and on the right hand side p occurs when p is not equal to a square, and* $(-1)^{\frac{1}{2}(s-1)}s$ *occurs when* $p = s^2 (s > 0)$. Jacobi has shown that a simple proof of the Fermat's theorem stating that every integer is a sum of four squares (see the notes to ch. IV, p. 000 and § 5 below), may be deduced from this theorem.

In § 5 we shall give a proof of the Jacobi theorem by Liouville's method.

§ 3. The Ramanujan theorem [1]

Ramanujan (see [72], p. 211) conjectured the following interesting property of function $\bar{\mu}(n)$:

THEOREM 21. *If r is an integer, whose only prime factors are 5, 7 and 11, (i.e. $r = 5^a 7^b 11^c$, $a \geqq 0$, $b \geqq 0$, $c \geqq 0$) then for every $n > 0$ satisfying the congruence $24n \equiv 1 \pmod{r}$, we have $\bar{\mu}(n) \equiv 0 \pmod{r}$.*

First, let us note that the truth of Ramanujan's conjecture is established if it is proved separately for moduli $r_1 = 5^a$, $r_2 = 7^b$, $r_3 = 11^c$. There still is no complete proof of this conjecture[1]. Ramanujan himself, and subsequently other authors, have proved this theorem only for the cases $a = 1, 2, 3$, $b = 1, 2$, $c = 1$ (see Ramanujan [72], p. 211). Their method of proof is analytical, and is based on the properties of some modular equations. The exposition of the proofs may be found in paper by Krečmar [34].

For the cases $r = 5$ and $r = 7$ Ramanujan's theorem may be proved by arithmetical methods based on theorems on partitions given in the preceeding sections. Let r be a prime, and let n be a given integer; by formulae (8) § 2, it is easy to obtain the following expression for $\bar{\mu}(n)$:

$$\bar{\mu}(n) = N((-1)^{m_1+m_2+\ldots+m_{r-1}};$$
$$n = \sum a^* + \sum a_1^* + \sum a_2^* + \ldots + \sum a_{r-1}^* + \sum_{m_1} b_1 + \sum_{m_2} b_2 + \ldots + \sum_{m_{r-1}} b_{r-1}) \quad (18)$$

where $\sum a^*, \sum a_1^*, \ldots$ are the sums in which some terms may repeat, and $\sum_{m_1} b_1, \sum_{m_2} b_2, \ldots$ are the sums of $m_1, m_2, \ldots$ distinct parts; each of these sums may be absent. In fact, collecting on the right hand side of (18) the terms for which expressions $\sum a_1^* + \sum_{m_1} b_1 = u_1$, $\sum a_2^* + \sum_{m_2} b_2 = u_2, \ldots$ have the same systems of values, we find

[1] This theorem is, in fact, a conjecture which has now been proved shown to be incorrect. Watson has provided a corrected form $\mu(n) \equiv 0 \pmod{5^\alpha 7^\beta 11^c}$ where $\beta = [\frac{1}{2}(b+2)]$, and proved this for general a, b and $c \leq 2$. See Hardy and Wright (1959) Introduction to the theory of numbers, p. 289.

that this part of the sum (18) is equal to the product of sums $N((-1)^{m_i}; u_i = \sum a_i^* + \sum_{m_i} b_i)$ $(i = 1, 2, \ldots, r-1)$ and, therefore, by (8), it is equal to zero in all cases apart from $u_1 = u_2 = \ldots = u_{r-1}$. Therefore, the value of the sum (18) is $N(n = \sum a^*) = \bar{\mu}(n)$. Permuting cyclically the first r sums $\sum a^*, \sum a_1^*, \ldots, \sum a_{r-1}^*$ in the partition

$$n = \sum a^* + \sum a_1^* + \ldots + \sum a_{r-1}^* + \sum_{m_1} b_1 + \ldots + \sum_{m_{r-1}} b_{r-1} \tag{19}$$

we obtain from it $r-1$ more partitions. Since r is a prime, among r representations (19) which differ from each other by cyclic permutation of sums $\sum a^*, \ldots, \sum a_{r-1}^*$ the same representation can occur only when all sums $\sum a^*, \ldots, \sum a_{r-1}^*$ are identically the same, i.e. every term of one sum coincides with every term of the other. Therefore, from (18) we have $\bar{\mu}(n) \equiv N((-1)^{m_1+m_2+\ldots+m_{r-1}}$;

$$n = \sum_{m_1} b_1 + \sum_{m_2} b_2 + \ldots + \sum_{m_{r-1}} b_{r-1} + r \sum a^* \pmod r \tag{20}$$

Assume for every $n \geqq 0$

$$\varphi(n) = N((-1)^{m_1+m_2+\ldots+m_{r-1}}; n = \sum_{m_1} b_1 + \sum_{m_2} b_2 + \ldots + \sum_{m_{r-1}} b_{r-1}) \tag{21}$$

Then congruence (20) may be written as

$$\bar{\mu}(n) \equiv \psi(n) + \bar{\mu}(1)\psi(n-r) + \bar{\mu}(2)\psi(n-2r) + \ldots \pmod r \tag{22}$$

where on the right hand side the sum is continued as long as the argument of the function ψ remains non-negative. From (22), by means of inversion formula (12), we obtain

$$\psi(n) \equiv \sum_{r\omega_s \leqq n} (-1)^s \bar{\mu}(n - r\omega_s) \pmod r. \tag{23}$$

Congruences (22) and (23) show that if for every $n > 0$, satisfying the condition $n \equiv n_0 \pmod r$, we have $\psi(n) \equiv 0 \pmod r$, then the same property is possessed by function $\bar{\mu}(n)$ and conversely; therefore Ramanujan's theorem for module r is equivalent to the statement: $\psi(n) \equiv a \pmod r$ for every $n > 0$ for which $24n \equiv 1 \pmod r$. Applying the Euler-Legendre theorem in (21) we obtain for $\psi(n)$ the expression

$$\psi(n) = N((-1)^{\alpha_1+\alpha_2+\ldots+\alpha_{r-1}}; n = \omega_{\alpha_1} + \omega_{\alpha_2} + \ldots + \omega_{\alpha_{r-1}}),$$

which may be presented as

$$\psi(n) = N((-1)^{\alpha_1+\alpha_2+\ldots+\alpha_{r-1}};$$
$$24n+r-1 = (6\alpha_1-1)^2+(6\alpha_2-1)^2+\ldots+(6\alpha_{r-1}-1)^2). \quad (24)$$

To transform the obtained expression still further, we use the Jacobi theorem (17). Since the congruence $24n \equiv 1 \pmod r$ entering into Ramanujan's theorem excludes possibilities $r = 2$ and $r = 3$, we may assume that $r > 3$ and then $r \equiv 1$ or $r \equiv 2 \pmod 3$. Taking in the first case $r-1 = 3l$ we obtain from (24), by Jacobi's theorem,

$$\psi(n) = N((-1)^{\frac{1}{2}(s_1-1)}S_1 \cdot (-1)^{\frac{1}{2}(s_2-1)}s_2 \ldots (-1)^{\frac{1}{2}(s_l-1)}s_l;$$
$$8n+l = s_1^2+s_2^2+\ldots+s_l^2,\ s_i - \text{odd} > 0). \quad (25)$$

In the second case, when $r \equiv 2 \pmod 3$, we take $r-1 = 3l+1$ and obtain from (24)

$$\psi(n) = N((-1)^{\alpha-1}(-1)^{\frac{1}{2}(s_1-1)}s_1 \ldots (-1)^{\frac{1}{2}(s_l-1)}s_l;$$
$$24n+3l+1 = (6\alpha-1)^2+3s_1^2+3s_2^2+\ldots+3s_l^2,\ s_i - \text{odd} > 0). \quad (26)$$

The obtained expressions for $\psi(n)$ enable us to prove Ramanujan's theorem for the simplest cases $r = 5$ and $r = 7$. Namely, for $r = 5$ (26) gives

$$\psi(n) = \sum(-1)^{\frac{1}{2}(s-1)+\alpha-1} \cdot s,$$

where the summation is performed over all representations $24n+4 = (6\alpha-1)^2+3s^2$ (s odd, > 0); since $24n+4 \equiv 24n-1 \equiv 0 \pmod 5$ and since -3 is a quadratic non-residue of 5, it follows that in every representation $24n+4 = (6\alpha-1)^2+3s^2$ the numbers $6\alpha-1$ and s are divisible by 5, and consequently $\psi(n) \equiv 0 \pmod 5$. Similarly for $r = 7$ (25) gives

$$\psi(n) = \sum(-1)^{\frac{1}{2}(s-1)+\frac{1}{2}(t-1)}st,$$

where the summation is performed over all representations $8n+2 = s^2+t^2$ (s, t odd > 0). From the given congruence $24n \equiv 1 \pmod 7$ it follows again that $8n+2 \equiv 0 \pmod 7$ and therefore in every representation $8n+2 = s^2+t^2$ numbers s, t are divisible by 7, and consequently, $\psi(n) = 0 \pmod 7$ q.e.d.

The above method of proving Ramanujan's theorem is due to Uspensky.

§ 4. Liouville's methods; deduction of the fundamental identities

Over the period 1858–1865 Liouville published in his journal 18 short notes under the general title 'Sur quelques formules générales, qui peuvent être utiles dans la théories des nombres' (Articles I–XVIII) in which he gives without proof a series of arithmetical identities relating to arbitrary arithmetical functions. About these identities he writes that they are obtained by a very elementary methods (au moyen de l'algèbre la plus simple). At the same time in a large number of Liouville's notes many results which occur without proof are on the number of representations of an integer as a form of 3, 4, 5 and 6 variables, on the number of classes of binary forms, etc., with only a mention that all these results are obtained from his numerical identities. Though Liouville's results are concerned with forms of a particular kind (e.g. $x^2+y^2+z^2+2t^2$, $x^2+2y^2+3z^2+6t^2$ etc.) they exceed* the limits of the results of a general theory of quadratic forms of many variables in its present state, and therefore, they present a great interest. The methods used by Liouville have remained a mystery for a long time; only a small part of them has been proved by various authors by means of the theory of elliptic functions.

The reconstruction of the methods of Liouville we owe, in all its simplicity and complexity, to Uspensky. He did not only prove all the identities and results of Liouville's mentioned above, but he found many new similar formulae and applied them to the results found by various authors (Klein, Hirster, Humbert) by means of analytic methods (see J. Uspensky [63, 64, 65, 66]). Almost all Liouville's identities are corollaries of one fundamental identity which may be written as follows. Let $F(x, y, z)$ be an integral function, defined for all systems of values of three integral arguments x, y, z and satisfying only the conditions

$$F(-x, y, z) = -F(x, y, z)[\text{thus } F(0, y, z) = 0]$$
$$F(x, -y, -z) = F(x, y, z) \qquad (27)$$

Then the following formula holds

$$\sum_{m=h^2+\Delta\Delta'} F(\Delta+\Delta', h, \Delta-\Delta') = 2 \sum_{m=i^2+d\delta} F(\delta-2i, d+i, 2d+2i-\delta)+T. \qquad (28)$$

* This is no longer the situation due to Hecke "Analytische Arithmetic der Positiven quadratischen Formen". Denske Vid. Selsk. Math.-Fys. Medd. 17, no. 12, 134 pp. (1940).

Here $m > 0$ is a given integer, the sum on the left hand side is taken over all representations of m in the form $h^2+\Delta\Delta'$ ($h \gtrless 0$, $\Delta > 0$, $\Delta' > 0$ are integers), the sum on the right hand side is taken over all representations $m = i^2+d\delta$ with the same conditions for i, d, δ as for h, Δ, Δ'. Finally, $T = 0$ if m is not a square, and

$$T = \sum_{j=1}^{2s-1} \{F(2s, s-j, 2s-2j)-2F(j, s, j)\}, \tag{29}$$

if $m = s^2$ ($s > 0$). As usual, two representations $m = h^2+\Delta\Delta'$ $m = h_1^2+\Delta_1\Delta_1'$ are considered the same only for $h = h_1$, $\Delta = \Delta_1$, $\Delta' = \Delta_1'$; To prove (28) take

$$S = \sum_{m=i^2+d\delta} F(\delta-2i, d+i, 2d+2i-\delta),$$

and denote by S', S'', S''' the parts of this sum corresponding to representations $m = i^2+d\delta$ for which $2i+d-\delta > 0$, $2i+d-\delta < 0$, $2i+d-\delta = 0$, so that $S = S'+S''+S'''$. For every representation $m = i^2+d\delta$ in which $2i+d-\delta > 0$ take $i' = \delta-i$, $d' = 2i+d-\delta$, $\delta' = \delta$ then $m = i'^2+d'\delta'$, $d' > 0$, $\delta > 0$, $2i'+d'-\delta' = d > 0$, i.e. i', d', δ' is a representation of the same kind as i, d, δ. Noting that

$$\delta-2i = 2i'-\delta', \quad d+i = d'+i', \quad 2d+2i-\delta = 2d'+2i'-\delta'$$

and taking into account the properties (27) of function we obtain

$$S' = \sum_{2i+d-\delta>0} F(\delta-2i, d+i, 2d+2i-\delta)$$
$$= -\sum_{2i'+d'-\delta'>0} F(\delta'-2i', d'+i', 2d'+2i'-\delta') = -S' = 0$$

For every representation $m = i^2+d\delta$ in which $2i+d-\delta < 0$, take $h = d+i$, $\Delta = d$, $\Delta' = \delta-d-2i$; then h, $\Delta > 0$, $\Delta' > 0$, give a representation of m in the form $h^2+\Delta\Delta'$ for which $\Delta'-\Delta+2h = \delta > 0$, and we obtain

$$S'' = \sum_{2i+d-\delta<0} F(\delta-2i, d+i, 2d+2i-\delta)$$
$$= \sum_{m=h^2+\Delta\Delta',\ \Delta'-\Delta+2h>0} F(\Delta+\Delta', h, \Delta-\Delta').$$

Noting that in changing h, Δ, Δ' into $-h, \Delta', \Delta$ the expression under the last summation sign remains unchanged by (27), and the value $\Delta'-\Delta+2h$ changes sign, we can write

$$S'' = \tfrac{1}{2} \sum_{m=h^2+\Delta\Delta',\ \Delta'-\Delta+2h\neq 0} F(\Delta+\Delta', h, \Delta-\Delta'). \tag{30}$$

Finally, if we have $2i+d-\delta = 0$ for representation $m = i^2+d\delta$ then $m = (d+i)^2$; consequently, such representations may exist only if m is equal to a square. Taking $m = \delta^2$ $(s > 0)$ and noting that $\delta = 2i+d > 0$ yields $d+i > 0$, we obtain $d+i = s$, $i < s$, $\delta = 2i+d < 2s$. Thus, all representations i, d, δ which we have considered, are of the form $\delta-s$, $2s-\delta$, δ where integer δ runs through values 1, 2, 3, . . ., $2s-1$. Therefore, $S''' = 0$ for m not equal to a square, and

$$S''' = \sum_{\delta=1}^{2s-1} F(2s-\delta, s, 2s-\delta) = \sum_{j=1}^{2s-1} F(j, s, j)$$

for $m = s^2$. To obtain a final expression for sum S'' from (30) it remains to consider the sum $S_1 = \sum F(\Delta+\Delta', h, \Delta-\Delta')$, taken over representations $m = h^2+\Delta\Delta'$ for which $\Delta'-\Delta+2h = 0$. For such representations, we have

$$m = \left(\frac{\Delta+\Delta'}{2}\right)^2 = s^2, \quad \frac{\Delta+\Delta'}{2} = s > 0, \quad \frac{\Delta-\Delta'}{2} = h;$$

consequently, all the representations h, Δ, Δ' are of the form $\Delta-s$, Δ, $2s-\Delta$ where $\Delta = 1, 2, 3, \ldots, 2s-1$. Thus, $S_1 = 0$ for $m \neq s^2$ and

$$S_1 = \sum_{j=1}^{2s-1} F(2s, s-j, 2s-2j) \qquad \text{for } m = s^2,\ s > 0.$$

Moreover, (30) gives

$$S'' = \tfrac{1}{2} \sum_{m=h^2+\Delta\Delta'} F(\Delta+\Delta', h, \Delta-\Delta') - \tfrac{1}{2}S_1.$$

Substituting the expressions found for S', S'', S''' into $S = S'+S''+S'''$ we obtain the required identity (28). From identity (28) a series of new identities may be deduced by imposing various restrictions upon function $F(x, y, z)$. First, assume $F(x, y, z) = 0$ for even x (this restriction does not contradict the conditions (27)). Then (28) gives

$$\sum_{m=h^2+\Delta\Delta',\ \Delta+\Delta' \text{ odd}} F(\Delta+\Delta', h, \Delta-\Delta')$$

$$= 2 \sum_{\substack{m=i^2+d\delta \\ \delta \text{ odd}}} F(\delta-2i, d+i, 2d+2i-\delta) - 2\{ \sum_{\substack{j=1,3,5,\ldots,2s-1 \\ m=s^2,\ s>0}} F(j, s, j)\}, \tag{31}$$

where symbol $\{A\}_{m=s^2,\ s>0}$ denotes A for $m = s^2$ and 0 for m not equal to a square. Assuming the contrary true in (28), i.e. taking

$F(x, y, z) = 0$ for x odd, we leave only those terms in (28) for which the argument of function F is even. But then in all terms the third argument of F is even; taking thus $F(x, y, z) = \Phi(\frac{1}{2}x, y, \frac{1}{2}z)$ where Φ is a numerical function, satisfying only

$$\Phi(-x, y, z) = -\Phi(x, y, z), \Phi(x, -y, -z) = \Phi(x, y, z) \quad (32)$$

we obtain

$$\sum_{\substack{m=h^2+\Delta\Delta' \\ \Delta+\Delta' \text{ even}}} \Phi\left(\frac{\Delta+\Delta'}{2}, h, \frac{\Delta-\Delta'}{2}\right) = 2 \sum_{m=i^2+2d\delta} \Phi(d-i, \delta+i, \delta+i-d)$$

$$+\{\sum_{j=1}^{2s-1} \Phi(s, s-j, s-j) - 2\sum_{m=s^2, s>0}^{s-1} \Phi(j, s, j)\}. \quad (33)$$

Taking here $\Phi(x, y, z) = 0$ for y odd, and counting given number m as *odd*, we obtain

$$\sum_{m=4h^2+\Delta\Delta'} \Phi\left(\frac{\Delta+\Delta'}{2}, 2h, \frac{\Delta-\Delta'}{2}\right) = 2 \sum_{m=i^2+2d\delta,\ \delta \text{ odd}} \Phi(d-i, \delta+i, \delta+i-d)$$

$$+2\{\sum_{j=1, 3, 5, \ldots, 2s-1, m=s^2, s>0} \Phi(s, s-j, s-j) \quad (34)$$

Assuming the opposite true in (33), i.e. $\Phi(x, y, z) = 0$ for y even (again, assuming m odd), we obtain

$$\sum_{m=h^2+4\Delta\Delta'} \Phi(\Delta+\Delta', h, \Delta-\Delta') = 2 \sum_{m=i^2+4d\delta} \Phi(d+i, i-2\delta, i+d-2\delta)$$

$$+2\{\sum_{j=1, 3, 5, \ldots, s-2} \Phi(s, j, j) - \sum_{j=1}^{s-1} \Phi(j, s, j)\}.$$

If we assume here $m \equiv 1 \pmod 8$ and $\Phi(x, y, z) = 0$ for x-even, we obtain the following formula

$$\sum_{\substack{m=h^2+4\Delta\Delta' \\ \Delta+\Delta' \text{ odd}}} \Phi(\Delta+\Delta', h, \Delta-\Delta') = 2 \sum_{m=i^2+8d\delta} \Phi(2d+i, i-2\delta, i+2d-2\delta)$$

$$+2\{\sum_{j=1, 3, 5, \ldots, s-2, m=s^2, s>0} [\Phi(s, j, j) - \Phi(j, s, j)]\}. \quad (35)$$

In all these formulae function $\Phi(x, y. z)$ (or $F(x, y, z)$) has been assumed even over the set of two arguments y, z (see (27) and (32)); this condition is satisfied if we take $\Phi(x, y, z)$ to be odd over each argument y, z separately. Under this supposition, the left hand side in

formulae (28), (35) becomes zero (since h may be greater or less than zero). Thus, taking

$$F(-x, y, z) = F(x, -y, z) = F(x, y, -z) = -F(x, y, z) \quad (36)$$

$$\Phi(-x, y, z) = \Phi(x, -y, z) = \Phi(x, y, -z) = -\Phi(x, y, z) \quad (37)$$

we obtain, from (31) and (35)

$$\sum_{m=i^2+d\delta,\ \delta \text{ odd}} F(\delta-2i, d+i, 2d+2i-\delta) = \{\sum_{\substack{j=1,3,5,\ldots,2s-1 \\ m=s^2,\ s>0}} F(j, s, j)\} \quad (38)$$

$$\sum_{m=i^2+8d\delta} \Phi(i+2d, i-2\delta, i+2d-2\delta) = \{\sum_{j=1,3,5,\ldots,s-2,\ m=s^2,\ s>0} [\Phi(j, s, j)-\Phi(s, j, j)]\}. \quad (39)$$

These formulae yield many important identities of a more particular kind of function with one argument. First of all, taking in (34) $\Phi(x, y, z)$ to be equal first to $f(x)$ and then to $(-1)^{\frac{1}{2}y}f(x)$ where $f(x)$ is an odd function, we satisfy conditions (32), and obtain two formulae (m odd)

$$\sum_{m=4h^2+\Delta\Delta'} f\left(\frac{\Delta+\Delta'}{2}\right) = 2\sum_{m=i^2+2d\delta,\ \delta \text{ odd}} f(d+i) + \{sf(s)\}_{m=s^2,\ s>0}. \quad (40)$$

$$\sum_{m=4h^2+\Delta\Delta'} (-1)^h f\left(\frac{\Delta+\Delta'}{2}\right) = 2\sum_{m=i^2+2d\delta,\ \delta \text{ odd}} (-1)^{\frac{1}{2}(i-1)+\frac{1}{2}(\delta-1)} f(d+i) + \{(-1)^{\frac{1}{2}(s-1)}f(s)\}_{m=s^2,\ s>0}. \quad (41)$$

In (38) the first and the last arguments of function F are always odd, therefore we shall satisfy conditions (36) if we take $F(x, y, z) = (-1)^{\frac{1}{2}(x+z)+y}f(y)$ where $f(y)$ is an odd function. For every m we obtain

$$\sum_{m=i^2+d\delta,\ \delta \text{ odd}} (-1)^i f(d+i) = \{(-1)^{s-1}sf(s)\}_{m=s^2,\ s>0}. \quad (42)$$

Noting that in (39) all the arguments of function Φ are odd, assume $\Phi(x, y, z) = (-1)^{\frac{1}{2}(x+y+z-1)}\Phi(x, y)$ where $\Phi(x, y)$ is an *even* function:

$$\Phi(-x, y) = \Phi(x, -y) = \Phi(x, y) \quad (43)$$

we obtain for $m \equiv 1 \pmod 8$

$$\sum_{m=i^2+8d\delta} (-1)^{\frac{1}{2}(i-1)}\Phi(i+2d, i-2\delta) = \{(-1)^{\frac{1}{2}(s-1)} \sum_{j=1,3,5,\ldots,s-2,\ m=s^2,\ s>0} [\Phi(j, s)-\Phi(s, j)]\}. \quad (44)$$

A series of identities of another type follows from the main formula (28). Let $F(x)$ be an odd function and let $n > 0$ be a given integer. Apply formula (42) to number $m = n - d'\delta'$ ($d'\delta'$ are positive integers for which $n - d'\delta > 0$) assuming function $f(x)$ in this formula to be equal to $F(x-d') - F(x+d')$ which clearly is an odd function of x. We obtain

$$\sum_{n-d'\delta' = i^2 + d\delta,\ \delta \text{ odd}} (-1)^i \{F(d-d'+i) - F(d+d'+i)\} = \{(-1)^{s-1} s[F(s-d') - F(s+d')]\}.$$

Performing the summation for similar equalities for all systems of integer values d', δ' satisfying the conditions $d' > 0$, $\delta' > 0$, δ odd, $n - d'\delta' > 0$; on performing simplification on the right hand side, we obtain

$$\sum_{n = i^2 + d\delta + d'\delta',\ \delta,\ \delta' \text{ odd}} (-1)^i [F(d-d'+i) - F(d+d'+i)] = \sum_{n = i^2 + d\delta,\ \delta \text{ odd}} (-1)^i i F(i+d). \quad (45)$$

For further transformation we use formula (31); taking in it

$$F(x, y, z) = (-1)^{\frac{1}{2}(x+z)+y}(2y - z)F(y)$$

and

$$F(x, y, z) = (-1)^{\frac{1}{2}(x+z)+y} y F(y)$$

we obtain two formulae

$$\begin{aligned} 2\sum (-1)^i \delta F(d+i) &= \sum (-1)^{\Delta + h}(2h + \Delta' - \Delta)F(h) \\ &\quad + 2\{(-1)^{s-1} s^2 F(s)\} \\ 2\sum (-1)^i (d+i) F(d+i) &= \sum (-1)^{\Delta + h} h F(h) \\ &\quad + 2\{(-1)^{s-1} s^2 F(s)\}. \end{aligned} \quad (46)$$

Noting that

$$\sum_{n = h^2 + \Delta\Delta',\ \Delta + \Delta' \text{ odd}} (-1)^{\Delta + h} h F(h) = 0$$

$$\sum_{\substack{n = h^2 + \Delta\Delta' \\ \Delta + \Delta' \text{ odd}}} (-1)^{\Delta + h}(\Delta' - \Delta)F(h) = -2 \sum_{\substack{n = h^2 + d\delta \\ d \text{ even},\ \delta \text{ odd}}} (-1)^h (d - \delta) F(h) = -2 \sum_{n = i^2 + d\delta,\ \delta \text{ odd}} (-1)^i (d - \delta) F(i),$$

and subtracting formulae (46) from one another, we get

$$\sum (-1)^i i F(d+i) = \sum (-1)^i (\delta - d) F(d+i) + \sum (-1)^i (d - \delta) F(i).$$

Substituting this in (45), we finally obtain

$$\sum_{n=i^2+d\delta+d'\delta',\ \delta,\ \delta' \text{ odd}} (-1)^i[F(d-d'+i)-F(d-d'+i)]$$
$$= \sum_{n=i^2+d\delta,\ \delta \text{ odd}} (-1)^i[(\delta-d)F(d+i)+(d-\delta)F(i)]. \quad (47)$$

From this formula, as we shall prove presently, the following identity follows for every integer m, and for every even function $f(x)$

$$\sum_{\substack{m=d\delta+d'\delta' \\ \delta,\ \delta' \text{ odd}}} [f(d-d')-f(d+d')] = \sum_{m=d\delta,\ \delta \text{ odd}} (\delta-d)[f(d)-f(0)]. \quad (48)$$

In fact, for $m = 1$ this formula is obvious. Suppose that (48) is proved for all m less than some number n; in order to prove it true for n and for any even function, we use equality (47) which we write as follows

$$\sum_{n=d\delta+d'\delta',\ \delta,\ \delta' \text{ odd}} [F(d-d')-F(d+d')]$$
$$+ \sum_{i=1,2,\ldots n-i^2=d\delta+d'\delta',\ \delta,\ \delta' \text{ odd}} (-1)^i [F(d-d'+i)$$
$$+F(d-d'-i)-F(d+d'+i)-F(d+d'-i)]$$
$$= \sum_{n=d\delta,\ \delta \text{ odd}} (\delta-d)[F(d)-F(0)] \quad (49)$$
$$+ \sum_{i=1,2,\ldots} (-1)^i \sum_{n-i^2=d\delta,\ \delta \text{ odd}} \{(\delta-d)[F(d+i)+F(d-i)]$$
$$-(\delta-d)[F(i)+F(-i)]\}$$

For a given i the sums

$$\sum_{\substack{n-i^2=d\delta+d'\delta' \\ \delta,\ \delta' \text{ odd}}} [F(d-d'+i)+F(d-d'-i)-F(d+d'+i)-F(d+d'-i)]$$

and

$$\sum_{n-i^2=d\delta,\ \delta \text{ odd}} (\delta-d)[F(d+i)+F(d-i)-F(i)-F(-i)],$$

represent, in fact, the left and the right hand side of formula (48) written for number $m = n-i^2$ and for even function $f(x) = F(x+i)+F(x-i)$; these sums are equal to each other, since for $i = 1, 2, \ldots$, we have $n-i^2 < n$. Simplifying (49) we obtain (48) for number $m = n$. The following identities of a similar type are deduced in the same way (see Uspensky [64)], Premier Mém. I, § 2);

$$\sum_{2m=d\delta+d'\delta',\ d,\ \delta,\ d',\ \delta' \text{ odd}} [f(d-d')-f(d+d')]$$
$$= \sum_{m=d\delta,\ \delta \text{ odd}} d[f(0)-f(2d)], \quad f(x) \text{ even}, \quad (50)$$

$$\sum_{2m=d\delta+d'\delta',\ d,\ \delta,\ d',\ \delta' \text{ odd}} (-1)^{\frac{1}{2}(\delta-1)}[f(d+d')-f(d-d')] = \sum_{m=d\delta,\ \delta \text{ odd}} (-1)^{\frac{1}{2}(\delta-1)} d f(2d), \quad f(x) \text{ odd}, \quad (51)$$

$$\sum_{m=d\delta+d'\delta',\ \delta,\ \delta' \text{ odd}} (-1)^{\frac{1}{2}(\delta-1)}[f(d+d')-f(d-d')] = \sum_{m=d\delta,\ \delta \text{ odd}} (-1)^{\frac{1}{2}(\delta-1)} d f(d) - \sum_{m=d\delta,\ \delta \text{ odd}} \frac{1+(-1)^{\frac{1}{2}(\delta-1)}\delta}{2} f(d), \quad f(x) \text{ odd}, \quad (52)$$

$$2 \sum_{m=d\delta+2d'\delta',\ \delta' \text{ odd}} [f(d-2d')-f(d+2d')] = \sum_{m=d\delta} (\delta-d) f(d), \quad f(x) \text{ even} \quad (53)$$

$$2 \sum_{m=d\delta+2d'\delta',\ \delta' \text{ odd}} (-1)^{\frac{1}{2}(\delta'-1)}[f(d+2d')+f(d-2d')] = \sum_{m=d\delta} (-1)^{\frac{1}{2}(\delta-1)} d f(d) - \sum_{m=d\delta} f(d), \quad f(x) \text{ odd} \quad (54)$$

$$2 \sum_{m=d\delta+d'\delta',\ d \text{ odd}} [f(d-2d)-f(d+2d')] = \sum_{m=d\delta,\ \delta \text{ odd}} (4d-\delta+1) f(\delta) - 2 \sum_{m=d\delta,\ \delta \text{ odd}} [f(1)+f(3)+\ldots+f(\delta)] - 2 \sum_{m=d\delta} [f(1)+f(3)+\ldots+f(2\delta-1)], \quad f(x) \text{ even} \quad (55)$$

In the identities (53) and (54) the number m is assumed to be odd, in others – arbitrary. The assumption concerning function $f(x)$ are written separately for every identity.

§ 5. Representation of a number by a form in two, three or four variables

Consider the applications of Liouville's identities proved in the last section. First, we prove theorem of § 8, ch. II on the number of representations of an integer by means of simplest quadratic forms x^2+y^2, x^2+2y^2, x^2+3y^2. Choosing, for example, the form x^2+2y^2 let us denote the number of representations of an integer n by this form by $N(n)$ (where $N(0) = 1$). Assuming n odd, consider equation $n = i^2+4h^2+2k^2$. For a constant h the number of solutions of this equation is $N(n-4h^2)$, consequently, the total number of solutions of this equation is expressed by the sum $\sum N(n-4h^2)$ taken over all $h = 0, \pm 1, \pm 2, \ldots$ for which the argument of the function N remains positive. Evaluating the number of solutions of the same equation

$n = i^2+4h^2+2k^2$ by another method, namely for a constant i, we obtain, on comparing the results, a recurrence relation for function $N(n)$:

$$\sum_{i=\pm 1,\pm 3,\dots} N(n-i^2) = \sum_{h=0,\pm 1,\pm 2,\dots} N(n-4h^2). \tag{56}$$

Taking in (31) $F(x, y, z) = \sin \frac{1}{4}\pi x$ we get

$$\sum_{\substack{n=h^2+2\Delta\Delta' \\ \Delta \text{ odd}}} \sin \frac{\pi(\Delta+2\Delta')}{4} = \sum_{\substack{n=i^2+d\delta \\ \delta \text{ odd}}} \sin \frac{\pi(\delta+2i)}{4} - \left\{ \sum_{\substack{j=1,3,\dots,2s-1 \\ n=s^2,\, s>0}} \sin \frac{\pi j}{4} \right\},$$

or

$$\sum_{n=h^2+2\Delta\Delta',\, \Delta \text{ odd}} \left(\sin \frac{\pi\Delta}{4} \cos \frac{\pi\Delta'}{2} + \sin \frac{\pi\Delta'}{4} \cos \frac{\pi\Delta}{4} \right) + \left\{ \frac{1}{\sqrt{2}} \right\}_{n=s^2,\, s>0} = \sum_{n=i^2+d\delta,\, \delta \text{ odd}} \sin \frac{\pi\delta}{4} \cos \frac{\pi i}{2} \tag{57}$$

Let us note that for odd x

$$\sin \frac{\pi x}{2} = (-1)^{\frac{1}{2}(x-1)}, \qquad \cos \frac{\pi x}{2} = 0$$

$$\sin \frac{\pi x}{4} = \frac{1}{\sqrt{2}}(-1)^{\frac{1}{8}(x^2-1)+\frac{1}{2}(x-1)}, \qquad \cos \frac{\pi x}{4} = \frac{1}{\sqrt{2}}(-1)^{\frac{1}{8}(x^2-1)}$$

and assume $\psi(k) = \sum_{k=d\delta,\, \delta \text{ odd}} (-2/\delta)$, $\psi(0) = \frac{1}{2}$. Then the right hand side of (57) may be represented in the form

$$1/\sqrt{2} \sum_{h=0,\pm 1,\pm 2,\dots} (-1)^h \psi(n-4h^2).$$

Further, in the sum $\sum \sin \frac{1}{4}\pi\Delta \cos \frac{1}{2}\pi\Delta'$ on the left hand side, only those terms remain which have Δ' even, consequently, this sum has a value distinct from zero only for $n \equiv 1 \pmod 4$ and then

$$\sum_{\substack{n=h^2+2\Delta\Delta' \\ \Delta \text{ odd}}} \sin \frac{\pi\Delta}{4} \cos \frac{\pi\Delta'}{2} + \left\{ \frac{1}{\sqrt{2}} \right\}_{n=s^2,\, s>0}$$

$$= \frac{1}{\sqrt{2}} \sum_{\substack{n=i^2+\Delta\Delta' \\ \Delta \text{ odd}}} (-1)^{\Delta'} \left(\frac{-2}{\Delta} \right) + \left\{ \frac{1}{\sqrt{2}} \right\}_{n=s^2,\, s>0}$$

$$= \frac{1}{\sqrt{2}}(-1)^{\frac{1}{4}(n-1)} \sum_{i=\pm 1,\pm 3,\dots} \psi(n-i^2),$$

where in the last sum the summation is performed over all odd i for which the argument ψ remains greater or equal to zero. Similarly, the sum $\sum \sin \frac{1}{2}\pi\Delta' \cos \frac{1}{4}\pi\Delta$ is present only when $n \equiv 3 \pmod 4$ and, in this case, it is equal to $(1/\sqrt{2})(-1)^{\frac{1}{4}(n-3)} \cdot \sum_{i=\pm 1, \pm 3, \ldots} \psi(n-i^2)$. Thus, (57) gives

$$\varepsilon \sum_{i=\pm 1, \pm 3, \ldots} \psi(n-i^2) = \sum_{h=0, \pm 1, \pm 2, \ldots} (-1)^h \psi(n-4h^2),$$

where $\varepsilon = (-1)^{\frac{1}{4}(n-1)}$ for $n \equiv 1$ and $\varepsilon = (-1)^{\frac{1}{4}(n-3)}$ for $n \equiv 3 \pmod 4$. Taking into account the fact that $\psi(n) = 0$ for $n \equiv 5, 7 \pmod 8$, it is easy to transform the obtained relation into

$$\sum_{i=\pm 1, \pm 3, \ldots} \psi(n-i^2) = \sum_{h=0, \pm 1, \pm 2, \ldots} \psi(n-4h^2). \tag{58}$$

Comparing (56) and (58) gives for every k the equality $N(k) = 2\psi(k)$ which we wish to prove. In fact, assuming the equality true for all odd k, less than n, we conclude, by obvious relations $\psi(2m) = \psi(m)$, $N(2m) = N(m)$ that it is true also for all even k less than n and then (56) and (58) give $N(n) = 2\psi(n)$, q.e.d. Taking in (42) $f(x) = \sin \frac{1}{2}(\pi x)$ we obtain

$$\sum_{m=i^2+d\delta,\ \delta \text{ odd}} (-1)^i \sin \frac{\pi d}{2} \cos \frac{\pi i}{2} = \left\{(-1)^{s-1} s \sin \frac{\pi s}{2}\right\}_{m=s^2,\ s>0},$$

or, considering m odd

$$\sum_{m=4h^2+d\delta} (-1)^{h+\frac{1}{2}(\delta-1)} = \{(-1)^{\frac{1}{2}(s-1)} s\}_{m=s^2,\ s>0}.$$

Applying to the left hand side the theorem on the number of representations of a number by form x^2+y^2 (§ 8, ch. II, formula (34)), we obtain the following useful Liouville's theorem:

THEOREM 22. *For every odd m the following equality holds*:

$$\sum_{m=i^2+4k^2+4h^2,\ i>0} (-1)^h = \{(-1)^{\frac{1}{4}(s-1)} s\}_{m=s^2,\ s>0}. \tag{59}$$

Such 'well simplifiable' sums as the one on the left hand side of (59) (or in Jacobi theorem (17) § 2) are of great importance in determining the number of representations by forms in four and more variables. Taking in (42) $f(x) = \sin \frac{1}{4}\pi x$ we find

$$\sum_{m=i^2+d\delta,\ \delta \text{ odd}} (-1)^i \sin \frac{\pi d}{4} \cos \frac{\pi i}{4} = \left\{(-1)^{s-1} s \sin \frac{\pi s}{4}\right\}_{m=s^2,\ s>0}.$$

Assume $m \equiv 3 \pmod 8$ then the right hand side is zero, the left hand side we split into two sums corresponding to even and odd values of i. We obtain

$$\sum_{m=16h^2+d\delta} (-1)^h \left(\frac{-2}{d}\right) = \sum_{m=i^2+2d\delta} (-1)^{\frac{1}{8}(i^2-1)} \left(\frac{-1}{d}\right).$$

Applying the theorems on the number of representations by the forms x^2+2y^2 and x^2+y^2.

We obtain:

$$\sum_{m=i^2+2k^2+16h^2} (-1)^h = \sum_{m=i^2+2k^2+8l^2} (-1)^{\frac{1}{8}(i^2-1)} \tag{60}$$

Noting that the number k in both representations $m = i^2+2k^2+16h^2$ and $m = i^2+2k^2+8l^2$ is odd and, consequently, $n = m-2k^2 \equiv 1 \pmod 8$, we obtain from (60) by the induction method the following theorem of Gauss-Jacobi: *for every integer n of the form* $8k+1$ *the representation by forms* x^2+y^2 *and* x^2+2y^2 *are related in such a way that*

$$\sum_{m=i^2+16h^2} (-1)^h = \sum_{m=j^2+8l^2} (-1)^{\frac{1}{8}(j^2-1)}. \tag{61}$$

For the case of a prime n this theorem has already been obtained in ch. III in comparing the criteria of the biquadratic character of 2 (§ 3, ch. III, theorem 1).

Consider the ternary forms. We must note that the number of representations by them (and, in general by forms with an odd number of variables) are obtained by Liouville's methods with much more difficulty than for the forms with an even number of variables. The few ternary forms, number of representations by which may be determined by Liouville's methods, are given in Uspensky's [66] paper. An example of such investigation is given in § 2, ch. VI (for a form $x^2+y^2+z^2$); here we restrict ourselves to proving Jacobi's theorem formulated above (§ 2, formula (17)). Taking in (44) $\Phi(x, y) = \cos \frac{1}{3}(2\pi x)$ we obtain, for $m \equiv 1 \pmod 8$,

$$\sum_{m=i^2+8d\delta} (-1)^{\frac{1}{2}(i-1)} \sin\frac{2\pi i}{3} \sin\frac{2\pi d}{3} = \{(-1)^{\frac{1}{2}(s-1)}\varepsilon\}_{m=s^2,\, s>0}, \tag{62}$$

where $\varepsilon = -\frac{1}{2}s, \frac{1}{4}s-\frac{1}{4}$ or $\frac{1}{4}s+\frac{1}{4}$ according as $s \equiv 0, 1$ or $-1 \pmod 3$. Consider the sum $\sigma = \sum_{4k=d\delta} \sin \frac{2}{3}\pi d$ where $k > 0$ is a given integer. Noting that $\sin \frac{1}{3}(2\pi x) - \frac{1}{2}\sqrt{3}(x/3)$ or (for odd $x > 0$) $= \frac{1}{2}\sqrt{3}(-3/x)$ we

collect in σ the terms with the same highest power of 2 entering d. Then, taking $k = 2^{\alpha}l$ ($\alpha \geqq 0$, l odd), we find that $\sigma = 0$ for odd α and $\sigma = \frac{1}{2}\sqrt{3}\sum_{l=d\delta}(-3/d)$ for even α. Remembering the result of § 8, ch. II (formulae (38) and (39)) on the number of representations by form x^2+3y^2 we can write in all cases

$$\sigma = \frac{\sqrt{3}}{12} N(4k = x^2+3y^2).$$

Substituting this in (62), and transferring the necessary terms from the right hand side to the left if $m = s^2$, we finally obtain

$$\sum_{m=i^2+2j^2+6k^2} (-1)^{\frac{1}{2}(i-1)} \left(\frac{i}{3}\right) = \{2(-1)^{\frac{1}{2}(s-1)}s\varepsilon'\}, \qquad (63)$$
$$m=s^2,\ s>0$$

where $\varepsilon' = 1$ for $s \not\equiv 0$ and $s' = -2$ for $s \equiv 0 \pmod 3$. The sum on the left hand side may be represented in the form $2\sum(-1)^{\frac{1}{2}(i-1)}$ on adjoining to the equation $m = i^2+2j^2+6k^2$ an additional condition $i \equiv 1 \pmod 3$. Noting that for $m \equiv -1 \pmod 3$ there exist no representations with $i \equiv 1 \pmod 3$, that $j = 0 \pmod 3$ for $m \equiv 1$, and $j \not\equiv 0 \pmod 3$ for $m \equiv 0$, we easily transform (63) into

$$\sum_{m=i^2+2j^2+6k^2,\ i-j+1=0 \pmod 3} (-1)^{\frac{1}{2}(i+1)} = \{(-1)^{\frac{1}{2}(s-1)}s\}. \qquad (64)$$
$$m=s^2,\ s>0$$

Let us note that apart from condition $i-j+1 \equiv 0 \pmod 3$ the numbers i, j, k in representation $m = i^2+2j^2+6k^2$ satisfy the condition $j+k \equiv 0 \pmod 2$, which follows from the assumption that $m \equiv 1 \pmod 8$ (see above). Therefore, the numbers corresponding to i, j, k by formulae $i = 2\alpha+2\beta+2\gamma-1$, $j = 2\alpha-\beta-\gamma$, $k = \beta-\gamma$ are *integers* α, β, γ and from $m = i^2+2j^2+6k^2$ we obtain for these integers the following relation

$$3m = (6\alpha-1)^2+(6\beta-1)^2+(6\gamma-1)^2.$$

Formula (64) transforms into Jacobi theorem

$$\sum_{3m=(6\alpha-1)^2+(6\beta-1)^2+(6\gamma-1)^2} (-1)^{\alpha+\beta+\gamma} = \{(-1)^{\frac{1}{2}(s-1)}s\}.$$
$$m=s^2,\ s>0$$

Identity (44) from which we deduced Jacobi theorem allows us also to prove Euler's formula for the sum of divisors $\zeta(n)$ (see (7), § 1) Without going into details we just mention that taking in (44) $m = 24n+1$ and $\Phi(x, y) = x \sin \frac{1}{3}(2\pi x)(2+\frac{1}{3}2\pi y)$ the left hand side of

(44) may be represented as the sum of two quantities

$$S = \sum_{24n+1=i^2+8d\delta} (-1)^{\frac{1}{2}(i+1)} i \left(2\cos\frac{2\pi i}{3} + \cos\frac{2\pi\delta}{3}\right) \sin\frac{2\pi d}{3}$$

and

$$T = \sum_{24n+1=i^2+8d\delta} (-1)^{\frac{1}{2}(i+1)} d \sin\frac{2\pi i}{3} \cos\frac{2\pi d}{3} \left(\cos\frac{2\pi\delta}{3} - 4\right).$$

But it is easy to see that

$$S = 0, \quad T = 12 \sum (-1)^{\frac{1}{2}(i-1)} \sin\frac{2\pi i}{3} \zeta\left(\frac{24n+1-i^2}{24}\right),$$

from which we obtain Euler's formula (7).

The simplest quadratic form in four variables is $x^2+y^2+z^2+t^2$. The number of representations by this form is determined by means of the following Jacobi theorem:

THEOREM 23. *The number of representations of every integer $m > 0$ as a sum of four squares is equal to eight times the sum of all divisors of m when m is odd, and 24 times the sum of all odd divisors of m when m is even.*

This theorem can be proved by the same method which has been applied above to the form x^2+2y^2. However, we shall not pause for it here, as it will be proved in the next section. For $m \equiv 1 \pmod 4$ in the representation $m = x^2+y^2+z^2+t^2$ one of the numbers x, y, z, t is odd and the remaining ones are even. Therefore, theorem 23 gives

$$N(m = x^2+4y^2+4z^2+4t^2) = 2\zeta(m).$$

But, by theorem 22 of Liouville

$$\sum_{m=x^2+4y^2+4z^2+4t^2} (-1)^t = 2 \sum_{m=i^2+4k^2,\, i>0} (-1)^{\frac{1}{2}(i-1)} i.$$

Adding this with the preceeding equality, we obtain for $m \equiv 1 \pmod 4$

$$N(m = x^2+4y^2+4z^2+16t^2) = \zeta(m) + \sum_{m=i^2+4k^2,\, i>0} (-1)^{\frac{1}{2}(i-1)} i. \quad (65)$$

Identities of another type deduced in § 4 (see formulae (50)–(55)) also enable us to obtain the numbers of representations by forms in

four variables. For example, in order to determine the number of representations by a form $x^2+y^2+z^2+2t^2$ assume in (55) $f(x) = \cos \frac{1}{4}\pi x$, then we obtain

$$4 \sum_{n=d\delta+d'\delta',\, d \text{ odd}} \sin\frac{\pi d}{4} \sin\frac{\pi d'}{2} = \frac{1}{\sqrt{2}} \sum_{n=d\delta,\, \delta \text{ odd}} (4d-\delta+1)\left(\frac{2}{\delta}\right)$$
$$-2 \sum_{=d\delta,\, \delta \text{ odd}} \left[\cos\frac{\pi}{4} + \cos\frac{3\pi}{4} + \ldots + \cos\frac{\delta\pi}{4}\right]$$
$$-2 \sum_{n=d\delta} \left[\cos\frac{\pi}{4} + \cos\frac{3\pi}{4} + \ldots + \cos\frac{(2\delta-1)\pi}{4}\right],$$

or, on simplifying

$$8 \sum_{n=d\delta+d'\delta',\, d,\, d' \text{ odd}} (-1)^{\frac{1}{2}(d'-1)} \left(\frac{-2}{d}\right) = 2 \sum_{n=d\delta,\, \delta \text{ odd}} (4d-\delta+1)\left(\frac{2}{\delta}\right)$$
$$-4 \sum_{n=d\delta,\, \delta \equiv 1 \pmod 4} (-1)^{\frac{1}{2}(\delta-1)} - 4 \sum_{n=d\delta,\, \delta \text{ odd}} (-1)^{\frac{1}{2}(\delta-1)}.$$

Applying the theorems on representations by forms x^2+y^2, x^2+2y^2 we find that the left hand side of this equality is, in fact

$$N(n = x^2+y^2+z^2+2t^2,\ x^2+y^2 > 0,\ z^2+2t^2 > 0)$$

therefore, to obtain the total number of representations by a form $x^2+y^2+z^2+2t^2$ we must add to the left hand side the terms

$$N(n = x^2+y^2) + N(n = z^2+2t^2)$$
$$= 4 \sum_{n=d\delta,\, \delta \text{ odd}} (-1)^{\frac{1}{2}(\delta-1)} + 2 \sum_{n=d\delta,\, \delta \text{ odd}} \left(\frac{-2}{\delta}\right).$$

Then the right hand side, on simplifying, becomes

$$2 \sum_{m=d\delta,\, \delta \text{ odd}} (4d-\delta)\left(\frac{2}{\delta}\right).$$

Taking $n = 2^\alpha m$ ($\alpha \geqq 0$, m odd) and introducing a numerical function

$$\omega(m) = \sum_{m=d\delta} d\left(\frac{2}{\delta}\right),$$

we finally obtain (Liouville [48])

$$N(n = x^2+y^2+z^2+2t^2) = 2\left(2^{\alpha+2}\left(\frac{2}{m}\right)\right)\omega(m),$$
$$n = 2^\alpha m, \quad \alpha \geqq 0, \quad m \text{ odd} \tag{66}$$

Here are some more similar results (Liouville [47, 49, 50, 51, 52])

$$N(2^\alpha m = x^2+y^2+3z^2+3t^2) = 4\cdot|2^{\alpha+1}-3|\cdot\sum_{m=d\delta,\ d\not\equiv 0 \pmod 3} d, \qquad \alpha \geqq 0, \quad m \text{ odd}. \tag{67}$$

$$N(m = x^2+8y^2+8z^2+64t^2) = \tfrac{1}{2}\zeta(m)+\tfrac{1}{2}\sum_{m=i^2+16s^2,\ i>0}(-1)^{\frac{1}{2}(i-1)}i+\sum_{m=r^2+8u^2,\ r>0}\left(\frac{-2}{r}\right)r, \qquad m \equiv 1 \pmod 8, \tag{68}$$

$$N(2^\alpha 3^\beta m = x^2+y^2+z^2+3t^2) = \left[3^{\beta+1}-(-1)^{\alpha+\beta}\left(\frac{m}{3}\right)\right]\left[2^{\alpha+1}+(-1)^{\alpha+\beta+\frac{1}{2}(m-1)}\right]\sum_{m=d\delta}(-1)^{\frac{1}{2}(\delta-1)}\left(\frac{\delta}{3}\right)d, \qquad \alpha \geqq 0, \quad \beta \geqq 0, \quad (m,6)=1 \tag{69}$$

$$N(2^\alpha m = x^2+2y^2+2z^2+2t^2+2u^2+2v^2) = \frac{2}{3}\left[4^{\alpha+1}-\left(\frac{-2}{m}\right)\right]\sum_{m=d\delta}\left(\frac{-2}{\delta}\right)d^2, \qquad \alpha \geqq 0, \quad m \text{ odd}, \tag{70}$$

$$N(2^\alpha 5^\beta m = x^2+y^2+5z^2+5t^2) = 2(5^{\beta+1}-3)\zeta(m), \qquad \alpha > 0, \quad \beta \geqq 0, \quad (m,10)=1 \tag{71}$$

In the first formula the sign $|\ |$ denotes the absolute value. The last formula gives the number of representations of an *even* number by a form $x^2+y^2+5z^2+5t^2$; it is interesting to note that neither Liouville nor his followers succeeded in determining the number of representations of an odd number by this form.*

§ 6. The number of representations of a number as a sum of 2, 4, 6, 8 and 10 squares

A beautiful application of Liouville's method is the problem of the representation of numbers as a sum of an even number of squares. After Jacobi had found the expression for the number of representations as a sum of four squares (theorem 23), the corresponding expressions for 6 and 8 squares were given by Eisenstein and also a partial result for 10 squares (see Bachmann [3], p. 652) for 10 and 12 squares they were found by Liouville. In 1914 V. Bulygin found

* See Lomadze, Acta Arith. 5 (1960), § 8.

a general analytic method for finding the number of representations by an even number of squares, and his evaluations went as far as 24 squares, thus proving the results of Eisenstein and Liouville. V. Bulygin's calculations need a very complicated apparatus of Jacobi θ-functions, whilst the solution of the same problem by Liouville's method, as was noted by Uspensky [63], does not need any additional methods apart from the basic formula (28) § 4. To point out all particular properties of the method and the results obtained, it suffices to prolong the evaluation up to 10 squares.

Denote by $N_p(m)$ the number of representations of a number m as a sum of p squares, i.e. the number of all solutions of an indeterminate equation $m = x_1^2+x_2^2+\ldots+x_p^2$ in integers $x_1, x_2, \ldots, x_p$ (so that $N_p(0) = 1$). It is easy to show that numerical function $N_p(m)$ satisfies for every m the relation

$$\sum_{i=0,\,\pm1,\,\pm2,\ldots} [m-(p+1)i^2]N_p(m-i^2) = 0 \qquad (72)$$

where the sum is taken over all i for which $m-i^2 \geqq 0$. In fact, let us write $N_{p+1}(m)$ equalities of the form $m = x_1^2+x_2^2+\ldots+x_{p+1}^2$ corresponding to all representations of m as a sum of $p+1$ squares, and add all these equalities. Then we obtain

$$mN_{p+1}(m) = \sum x_1^2+\sum x_2^2+\ldots+\sum x_{p+1}^2 = (p+1)\sum x_1^2. \qquad (73)$$

Combining in sum $\sum x_1^2$ the terms having the same value i^2 we note that there are $N_p(m-i^2)$ such terms. Therefore

$$\sum x_1^2 = \sum_{i=0,\,\pm1,\,\pm2,\ldots} i^2 N_p(m-i^2)$$

where the summation is performed over all i for which $i^2 \leqq m$. By a similar reasoning $N_{p+1}(m) = \sum_{i=0,\,\pm1,\,\pm2,\ldots} N_p(m-i^2)$. Substituting these expressions into (73) we obtain the required relation (72).

Relation (72) together with the condition $N_p(0) = 1$ does, clearly, define completely the value of the numerical function $N_p(m)$ for every $m \geqq 0$; thus, if a function $\Phi(m)$ is constructed, satisfying the same recurrence relation as (72) and condition $\Phi(0) = 1$, we have for every m

$$N_p(m) = \Phi(m).$$

In a nutshell, this is the idea of the present method. To construct such

functions we use Liouville's identities which follow from the fundamental identity (28). Taking in (38) $F(x, y, z) = (-1)^{\frac{1}{2}(z+1)+y}F(y, x)$ where $F(x, y)$ is an odd function in each argument x, y we obtain

$$\sum_{m=i^2+\delta d,\ \delta \text{ odd}} (-1)^{\frac{1}{2}(\delta-1)}F(d+i, \delta-2i)$$
$$= \{(-1)^{s-1} \sum_{j=1,3,5,\ldots,2s-1,\ m=s^2,\ s>0} (-1)^{\frac{1}{2}(j-1)}F(s, j)\} \quad (74)$$

The case of two squares. Taking in (74) $F(x, y) = xy$, we obtain, on simplifying

$$\sum_{m=i^2+d\delta,\ \delta \text{ odd}} (-1)^{\frac{1}{2}(\delta-1)}(d\delta-2i^2) = \{m\}.$$
$$m=s^2,\ s>0$$

On replacing on the left hand side $d\delta$ by $m-i^2$ and introducing an arithmetical function $\Phi(m) = 4\sum_{m=d\delta,\ \delta \text{ odd}}(-1)^{\frac{1}{2}(\delta-1)}$, $\Phi(0) = 1$ the latter equality may be rewritten as

$$\sum_{i=0,\pm1,\pm2,\ldots,i\leqq m} (m-3i^2)\cdot\Phi(m-i^2) = 0.$$

Comparing this with (72), we obtain $N_2(m) = \Phi(m)$ for every m. Thus, we have proved again the result of § 8, ch. II:

$$N(m = x^2+y^2) = 4\sum_{m=d\delta,\ \delta \text{ odd}} (-1)^{\frac{1}{2}(\delta-1)}.$$

The case of six squares. Taking in (74) first $F(x, y) = x^3y$ and then $F(x, y) = xy^3$ we obtain

$$\sum(-1)^{\frac{1}{2}(\delta-1)}d^2(m-7i^2)+\sum(-1)^{\frac{1}{2}(\delta-1)}(3mi^2-5i^4) = \{m^2\},$$
$$\sum(-1)^{\frac{1}{2}(\delta-1)}\delta^2(m-7i^2)+4\sum(-1)^{\frac{1}{2}(\delta-1)}(3mi^2-5i^4) = \{4m^2-3m\},$$

where all sums on the left hand sides are taken over the representations $m = i^2+\delta d$, δ odd, whilst the terms on the right hand sides correspond, as usual, to the case $m = s^2$. Eliminating the sum $\sum(-1)^{\frac{1}{2}(\delta-1)}(3mi^2-5i^4)$ from two preceeding equalities results in the formula

$$\sum(m-7i^2)(4d^2-\delta^2)(-1)^{\frac{1}{2}(\delta-1)} = \{3m\}$$

which may be represented in a form

$$\sum_{i=0,\pm1,\pm2,\ldots}(m-7i^2)\Phi(m-i^2) = 0,$$

taking

$$\Phi(m) = 4\sum_{m=d\delta,\ \delta \text{ odd}}(4d^2-\delta^2)(-1)^{\frac{1}{2}(\delta-1)}, \qquad \Phi(0) = 1.$$

Comparing the obtained formula with (72) we find, for every m

$$N_6(m) = \Phi(m).$$

Taking $m = 2^\alpha n$, $\alpha \geqq 0$, n odd we may represent the above result in the form

$$N_6(m) = 4[2^{2\alpha+2} - (-1)^{\frac{1}{2}(n-1)}] \sum_{m=d\delta,\ \delta \text{ odd}} (-1)^{\frac{1}{2}(\delta-1)} d^2; \qquad m = 2^\alpha n, \quad \alpha \geqq 0, \quad n \text{ odd}. \tag{75}$$

The case of ten squares. Taking in (74) successively $F(x, y) = x^5y = xy^5$, and $= x^3y^3$, we obtain, on simplifying, the following formulae

$$\sum (-1)^{\frac{1}{2}(\delta-1)} d^4(m-11i^2) + 10 \sum (-1)^{\frac{1}{2}(\delta-1)} d^2 i^2 (m-3i^2) + \sum (-1)^{\frac{1}{2}(\delta-1)} i^4 (5m-7i^2) = \{m^3\},$$

$$\sum (-1)^{\frac{1}{2}(\delta-1)} \delta^4 (m-11i^2) + 40 \sum (-1)^{\frac{1}{2}(\delta-1)} \delta^2 i^2 (m-3i^2) + 16 \sum (-1)^{\frac{1}{2}(\delta-1)} i^4 (5m-7i^2) = \{16m^3 - 40m^2 + 25m\},$$

$$3 \sum (-1)^{\frac{1}{2}(\delta-1)} i^2 (4d^2 + \delta^2)(m-3i^2) + \sum (-1)^{\frac{1}{2}(\delta-1)} [(m-3i^2)^3 - 12i^2(m-i^2)(m-3i^2)] = \{4m^3 - 3m^2\}.$$

Eliminating from these equations sums

$$\sum (-1)^{\frac{1}{2}(\delta-1)} d^2 i^2 (m-3i^2) \quad \text{and} \quad \sum (-1)^{\frac{1}{2}(\delta-1)} \delta^2 i^2 (m-3i^2),$$

we obtain

$$\sum (-1)^{\frac{1}{2}(\delta-1)} (16d^4 + \delta^4)(m-11i^2) + \sum (-1)^{\frac{1}{2}(\delta-1)} [32i^4(5m-7i^2) + 160i^2(m-i^2)(m-3i^2) - \tfrac{40}{3}(m-3i^2)^3] = \{-\tfrac{64}{3}m^3 + 25m\} \tag{76}$$

Denote the first and the last sums on the left hand side of this equality by P and Q respectively. Assuming

$$\chi(n) = \sum_{n=d\delta,\ \delta \text{ odd}} (-1)^{\frac{1}{2}(\delta-1)} (16d^4 + \delta^4), \qquad \chi(0) = \tfrac{5}{4},$$

we obtain for the first sum the expression

$$P - \{25m\} = \sum_{m=s^2,\ s>0 \quad i=0,\ \pm 1,\ \pm 2, \ldots,\ i^2 \leqq m} (m-11i^2)(m-i^2).$$

In the expression for the sum Q, we apply the theorem on the number of representations by a form x^2+y^2, then for Q we have

$$Q+\{\tfrac{64}{3}m^3\}_{m=s^2,\,s>0} = \sum_{m=i^2+j^2+k^2} [8i^4(5m-7i^2)+40i^2(m-i^2)(m-3i^2)-\tfrac{10}{3}(m-3i^2)^3].$$

Introducing under the summation sign instead of m its value $i^2+j^2+k^2$ we obtain

$$Q+\{\tfrac{64}{3}m^3\} = \sum [8i^4(5j^2+5k^2-2i^2) +40i^2(j^2+k^2)(j^2+k^2-2i^2)-\tfrac{10}{3}(j^2-k^2-2i^2)^3],$$

or, on simplifying

$$Q+\{\tfrac{64}{3}m^3\} = 4\sum_{m=i^2+j^2+k^2} (i^6-15i^4j^2+30i^2j^2k^2) \qquad (77)$$

We introduce an arithmetical function $\psi(n)$ defined for every n by an equality

$$\psi(n) = \sum_{n=j^2+k^2} (j^4-3j^2k^2).$$

Then, for this function we find

$$\sum_{i^2\leqq m} (m-11i^2)\psi(m-i^2) = \sum_{m=i^2+j^2+k^2} (m-11i^2)(j^4-3k^2j^2) = \sum_{m=i^2+j^2+k^2} (i^6-15i^4j^2+30i^2j^2k^2);$$

comparing this with (77) we finally obtain

$$Q+\{\tfrac{64}{3}m^3\}_{m=s^2,\,s>0} = 4\sum_{i=0,\,\pm1,\,\pm2,\ldots,\,i^2\leqq m} (m-11i^2)\psi(m-i^2).$$

Substituting the obtained expressions for sums P and Q into equality (76) and then assuming

$$\Phi(m) = \tfrac{4}{5}\chi(m)+\tfrac{16}{5}\psi(m), \qquad \Phi(0) = 1$$

we obtain

$$\sum_{i=0,\,\pm1,\,\pm2,\ldots,\,i^2\leqq m} (m-11i^2)\Phi(m-i^2) = 0,$$

from which it follows that, for every m, $N_{10}(m) = \Phi(m)$. Taking as usual $m = 2^\alpha n$ we may represent the latter expression for the number of representations as a sum of 10 squares in the following form

$$N_{10}(m)$$
$$= \tfrac{4}{5}(2^{4\alpha+4}+(-1)^{\frac{1}{2}(n-1)})\sum(-1)^{\frac{1}{2}(\delta-1)}d^4+\tfrac{16}{5}\sum_{m=j^2+i^2}(i^4-3i^2j^2)$$
$$m = 2^\alpha n, \quad \alpha \geqq 0, \quad n \text{ odd.} \quad (78)$$

Note that in this formula, together with a principal term which depends on the divisors of m there also occurs an additional term which is a sum $\sum(i^4-3i^2j^2)$ taken over all the representations of m by the form i^2+j^2. These additional terms appear in all subsequent formulae, expressing the number of representations as a sum of 12, 14, 16, ... squares. Their form becomes more complicated as the number of squares increases. For example, in the formula for the number of representations as a sum of 14 squares, the additional term present is a sum over all representations of a given number as a sum of 6 squares.

The case of four squares. Replacing $F(x, y, z)$ in (28) by $(-1)^x F(x, y, z)$ and adding the obtained formula to (28) we may represent the result in the following form

$$\begin{aligned}&2\sum((-1)^\delta+1)F(\delta-2i, d+i, 2d+2i-\delta)\\&\quad-\sum(1+(-1)^{d+\delta})F(d+\delta, i, d-\delta)\\&\quad=\{2\sum(1+(-1)^j)F(2s-j, s, 2s-j)\\&\quad-2\sum F(2s, s-j, 2s-2j)\}.\end{aligned} \quad (79)$$

The sums on the left hand side are taken over all representations $m = i^2+d\delta$, and the sums on the right hand side are present only when $m = s^2 (s > 0)$, and taken over $j = 1, 2, 3, \ldots$. Subtraction of the same formulae gives

$$\begin{aligned}&2\sum(1-(-1)^\delta)F(\delta-2i, d+i, 2d+2i-\delta)\\&\quad-\sum(1-(-1)^{d+\delta})F(d+\delta, i, d-\delta)\\&\quad=\{2\sum(1-(-1)^j)F(2s-j, s, 2s-j)\}.\end{aligned} \quad (80)$$

Since in (79) all the terms with odd arguments x and z of function $F(x, y, z)$ vanish, we may replace $F(x, y, z)$ in this formula by $(-1)^{\frac{1}{2}(x+z)}F(x, y, z)$ after which we obtain

$$\begin{aligned}&2\sum((-1)^d+(-1)^{d+\delta})F(\delta-2i, d+i, 2d+2i-\delta)\\&\quad-\sum((-1)^d+(-1)^\delta)F(d+\delta, i, d-\delta)\\&\quad=\{2\sum(1+(-1)^j)F(2s-j, s, 2s-j)\\&\quad-2\sum(-1)^jF(2s, s-j, 2s-2j)\}.\end{aligned}$$

Subtracting this formula from (80) we finally obtain

$$\sum \varepsilon(d, \delta)[F(\delta-2i, d+i, 2d+2i-\delta)-\tfrac{1}{2}F(d+\delta, i, d-\delta)]$$
$$= \{2\sum(-1)^{j-1}F(2s-j, s, 2s-j) + \sum(-1)^{j}F(2s, s-j, 2s-2j)\} \quad (81)$$

where it is assumed that $\varepsilon(d, \delta) = 1-(-1)^{d}-(-1)^{\delta}-(-1)^{d+\delta}$. This formula serves to determine the number of representations as a sum of 4, 12, 20,. . . squares in the same way as the previous formula served the same purpose in the case of 2, 6, 10, 14 squares. Taking $F(x, y, z) = xy^2$ for the simplest case of 4 squares in (81), we obtain, on simplifying

$$\sum_{m=i^2+d\delta} \varepsilon(d, \delta)(m-5i^2)d = \sum_{m=s^2,\, s>0} \{2m\} .$$

If we introduce a numerical function $\Phi(m) = 4\sum_{m=d\delta} \varepsilon(d, \delta)d$, $\Phi(0) = 1$ then the latter relation may be represented as

$$\sum_{i=0,\,\pm1,\,\pm2,\ldots,\,i^2\leqq m} (m-5i^2)\Phi(m-i^2) = 0,$$

Therefore $N_4(m) = \Phi(m)$ for every m. Noting that expression $\varepsilon(d, \delta) = -2$ for d and δ even, and $= 2$ otherwise, and combining in $\sum\varepsilon(d, \delta)$ the terms with the same highest power of 2 entering d, we easily obtain the final expression for $N_4(m)$:

$$N_4(m) = 8(2+(-1)^{m}) \sum_{m=d\delta,\ \delta \text{ odd}} \delta.$$

The result obtained is, in fact, the Jacobi theorem formulated in the previous section (theorem 23).

The case of eight squares. For this case, where the number of squares is divisible by 8, the role of the fundamental formula for construction of function $\Phi(m)$ is played by the fundamental formula (28) itself. Taking in it $F(x, y, z) = (-1)^{y}xy^4$ we obtain

$$\sum(-1)^{i+d}d^3(m-9i^2)+\sum(-1)^{i}i^4((-1)^{d}\delta-14(-1)^{d}d-d)$$
$$+6m\sum(-1)^{d+i}di^2 = \{(-1)^{m}(2m^3-2m^2+m)\} \quad (82)$$

where on the left hand side the sums are taken over the representations $m = i^2+d\delta$. Taking in (28) $F(x, y, z) = (-1)^{y}xy^3(2y-z)$, we find

$$3\sum(-1)^{i}i^4[7(-1)^{d}d-5(-1)^{d}\delta-2d]$$
$$-3m\sum(-1)^{i}i^2[8(-1)^{d}d-3(-1)^{d}\delta]$$
$$+3m^2\sum(-1)^{d+i}d = \{(-1)^{m}(4m^3-m^2)\} \quad (83)$$

But it is easy to verify that for every integer n

$$\sum_{n=d\delta}((-1)^d\delta-14(-1)^d d-d)+3\sum_{n=d\delta}(7(-1)^d d-5(-1)^d\delta-2d)=0;$$

Using this, we obtain from (82) and (83)

$$\sum(m-9i^2)(-1)^{i+d}d^3+9m\sum(-1)^i i^2((-1)^d\delta-2(-1)^d d)$$
$$+3m^2\sum(-1)^{d+i}d=\{(-1)^m(6m^3-3m^2+m)\}. \quad (84)$$

Again, taking in (28) $F(x, y, z)=(-1)^y xy^2$ we find

$$\sum(-1)^i i^2((-1)^d\delta-5(-1)^d d-d)$$
$$+m\sum(-1)^{i+d}d=\{(-1)^m(2m^2-m)\}.$$

This equality can be simplified similarly to the previous one, due to the remark that for every $n>0$

$$\sum_{n=d\delta}((-1)^d\delta-5(-1)^d d-d)=3\sum_{n=d\delta}((-1)^d\delta-2(-1)^d d),$$

and gives

$$3\sum(-1)^i i^2((-1)^d\delta-2(-1)^d d)+m\sum(-1)^{i+d}d=\{(-1)^m(2m^2-m)\}.$$

The relation obtained allows us to eliminate the two last sums in the left hand side of (84) on performing which we finally obtain

$$\sum(m-9i^2)(-1)^{i+d}d^3=\{(-1)^m m\}. \quad (85)$$

Introducing for every m an arithmetical function

$$\Phi(m)=16(-1)^m\sum_{m=d\delta}(-1)^d d^3, \qquad \Phi(0)=1,$$

we may represent (85) as

$$\sum_{i=0,\pm1,\pm2,\ldots,i^2\leq m}(m-9i^2)\Phi(m-i^2)=0$$

so that $N_8(m)=\Phi(m)$. From this we easily obtain the final expression for $N_8(m)$:

$$N_8(m)=16(-1)^m\frac{2^{3\alpha+3}-15}{7}\sum_{n=d\delta}d^3, \qquad m=2^\alpha n, \quad \alpha\geqq 0; \quad n \text{ odd}. \quad (86)$$

Notes to chapter 5

§ 1. Another purely arithmetical proof of Euler-Legendre theorem on pentagonal numbers belongs to Jacobi in his memoir: 'Beweis des Satzes, dass jede nicht fünfeckige Zahl ebenso oft in eine gerade als ungerade Anzahl verschiedener Zahlen zerlegt werden kann' (see [31], pp. 303–317).

Asymptotic expressions for additive functions $\lambda(n)$, $\bar{\mu}(n)$, $\nu(n)$ are given by Hardy and Ramanujan and independently by Uspensky. Note an interesting expression obtained by Uspensky:

$$\lim_{n\to\infty} \frac{\lambda(n)}{\nu(2n)} = \sqrt{2}.$$

§ 2. Ramanujan (see [72], p. 308) evaluated the table of values of functions $\bar{\mu}(n)$ up to $n = 200$.

Using the Vahlen theorem formulated in the text, we can deduce many more recurrence relations for the functions even more convenient for evaluation of values of these functions than formulae (13) and (15):

$$\sum (-1)^h \lambda(n-2\omega_h) = \{1\}_{n=\frac{1}{2}(s^2-s),\, s>0}, \tag{87}$$

$$\sum (-1)^h \lambda(n-h^2) = \{(-1)^s\}_{n=\omega_s}, \tag{88}$$

$$\sum (-1)^h \lambda(n-2h^2) = \{(-1)^{\frac{1}{2}(s^2-s)}\}_{n=\omega_s}, \tag{89}$$

$$\sum (-1)^h \lambda(n-3h^2) = \{1\}_{n=\omega_s}, \tag{90}$$

$$\sum (-1)^h \nu(n-\omega_h) = \{2(-1)^s\}_{n=2s^2,\, s>0}, \tag{91}$$

$$\sum (-1)^h \nu(n-4\omega_n) = \{1\}_{n=\frac{1}{2}(s^2-s),\, s>0}. \tag{92}$$

Applying to (91) inversion formula (12) given in the text, we obtain an expression of $\nu(n)$ through function $\bar{\mu}(n)$:

$$\nu(n) = \sum (-1)^h \bar{\mu}(n-2h^2). \tag{93}$$

§ 5. In § 3, ch. III in defining the biquadratic character of 2, we obtained a relation between representations of a prime $p \equiv 1 \pmod 8$

by forms x^2+8y^2 and x^2-8y^2. For a composite number $n \equiv 1 \pmod 8$ this relation is expressed by *Smith's theorem*:

$$\sum_{n=x^2+8y^2,\, x>0} (-1)^y = \sum_{n=x^2-8y^2,\, x+4y>0,\, x-4y>0} (-1)^{\frac{1}{4}(x-1)+y}$$

which is proved similarly to (61) in the text.

Taking $f(x) = x$ in formula (42), we obtain

$$\sum_{i=0,\,\pm 1,\,\pm 2,\ldots,\, i^2 \leqq n} (-1)^i \sigma(n-i^2) = \{(-1)^{n-1} n\}$$

where $\sigma(m)$ denotes arithmetical function $\sum_{m=d\delta,\, \delta \text{ odd}} d$. When n is a prime p of form $4k+1$ this gives

$$\sigma(p-1^2)-\sigma(p-2^2)+\sigma(p-3^2)-\ldots = \frac{p+1}{2}. \qquad (94)$$

It is easy to verify that $\sigma(m)$ is odd if and only if the argument m is an odd square, and since in the right hand side of (94) stands an odd number, we see that there exists a number i for which $p-i^2$ is an odd square. Thus, we obtain the Fermat theorem that a prime $p = 4k+1$ is a sum of two squares; the fact that this representation is unique is proved in a usual way. This fairly simple proof of Fermat's theorem is taken from an unpublished manuscript of the late mathematician K. M. Semenov.

Arithmetic of quaternions (see Venkov [95]) allows us to establish that Liouville's theorem (see (59)) and the Jacobi theorem (equality (17)) proved in § 5, and other theorems of a similar kind, present simple consequences of Gauss's theorem on genera (§ 12, ch. IV).

§ 6. For representation of *binary* forms as a sum of several linear functions with integer coefficients, see Mordell [61]. In this paper Mordell establishes the conditions for a binary form to be representable as a sum of 2, 3, 4 and 5 squares. It may be noted that the case of 5 squares needs no restrictions so that every positive binary form is a sum of 5 squares of linear functions with integer coefficients.

As a generalisation of a problem on representation of a number as a sum of squares, we may consider the famous *Waring theorem*: *every integer greater than zero may be represented as a sum of no more than g_p p-the powers of natural numbers*, where p is an integral exponent, and g_p depends only on p and not on the number which is

being represented. This fact was formulated by Waring in 1782 as a conjecture and was a subject of many researches (of analytical nature) during the last 20 years, there still is no elementary proof of it.* Recently (may 1934) an important paper appeared, by akad. I. M. Vinogradov [91], in which he gives inequality $g_p < 32\ (p \log p)^2$, and thus lowers considerably the previous upper limit for the number g_p [1].

---

[1] I. M. Vinogradov has shown that

$$g_n = O(n \log n)$$

In 1942 Linnik proved $g_3 \leqq 7$, Davenport proved $g_4 = 16$, $g_5 \leqq 23$.

For all $n \geqq 2$ we have $g_n \geqq n+1$, so that the estimate $g_n = O(n \log n)$ cannot be greatly improved.

I. M. Vinogradov has shown that

$$g_n < n(3 \log n+11)$$

Dun Huan Chan used Vinogradov's method to obtain the estimates

$$g_n < n(3 \log n+9) \quad \text{for } n = 2^k \text{ and}$$
$$g_n < n(3 \log n+7) \quad \text{for } n \neq 2^k.$$

Later Vinogradov improved his estimate to:

$$g_n/n < 2 \log n+4 \log \log n+2 \log \log \log n+13$$

(Izvestia Akad. Nauk, 23 (1959) 613–642).

* Elementary proof was found by Linnik. It may be found in Khintchin "Three pearls of number theory", chapter IV.

6. THE CLASS NUMBER OF BINARY QUADRATIC FORMS

The present chapter contains all that can be proved (at the present state of knowledge) by elementary methods, concerning the most important numerical function – the number of classes of binary quadratic forms of negative determinant.

§ 1. Tables of the class numbers. Regular determinants

In the present section we give some information tables which may may be obtained from the existing tables of class numbers. Such tables were evaluated by Gauss [19]; they provide the number of properly primitive (positive) classes of forms for all negative determinants from -1 to -3000 and for all positive determinants from 1 to 300. Moreover, Gauss evaluated the numbers of classes for all determinants lying in intervals[1] $(-4300, -4200)$, $(-5100, -5000)$, $(-6300, -6000)$, $(-10000, -9000)$, $(-12000, -11700)$, $(+800, +1000)$. If κ is the number of genera, and λ – the number of classes in every genus for a given determinant d (we consider always classes which are properly primitive and positive for $d < 0$), then the total number of classes is $\kappa\lambda$ (§ 12, ch. IV). The quantity κ is a power of two easily definable by the number of distinct prime divisors of d (§ 12, ch. IV, theorem 16); In Gauss's table the determinants inside every hundred are situated according to the increase of κ. We write κ in Roman numerals, and λ in Arab numerals. The pair of numbers κ,λ is called the classification of determinant d. For example, for determinant -16 the classification is II, 1.

The first question in considering the table of the class numbers is: what are the determinants with the same classification. It seems likely that a series of such determinants always stops at some point,

---

[1] All these separate tables of numbers of classes published in the volume II of Gauss's complete works present, possible, only fragments of one general table which has not reached us entirely.

i.e. that there exists a finite number of determinants with a given number of classes. However, to show this proposition is, obviously,* very difficult. To give an example, we write all negative determinants of Gauss's table with simple qualifications I, 1; I, 3, II, 1, etc.:

I, 1	1, 2, 3, 4, 7.
I, 3	11, 19, 23, 27, 31, 43, 67, 163.
I, 5	47, 79, 103, 127.
I, 7	71, 151, 223, 343, 463, 487.
II, 1	5, 6, 8, 9, 10,12, 13, 15, 16, 18, 22, 25, 28, 37, 58.
II, 2	14, 17, 20, 32, 34, 36, 39, 46. 49, 52, 55, 63, 64, 73, 82, 97, 100, 142, 148, 193.
IV, 1	21, 24, 30, 33, 40, 42, 45, 48, 57, 60, 70, 72, 78, 85, 88, 93, 102, 112, 130, 133, 177, 190, 232, 253.
VIII, 1	105, 120, 165, 168, 210, 240, 273, 280, 312, 330, 345, 357, 385, 408, 462, 520, 760.
XVI, 1	840, 1320, 1365, 1848.

For every classification on the right, the absolute values of determinants having this classification are written on the left. The classification I, 2; I, 4 do not exist at all, since in the case of the existence of only one genus the number of classes in this genus is odd (§ 10, ch. IV). Further, it is interesting that in Gauss's table the negative determinants have no classification of the form κ, 1 where $\kappa \geqq 32$ (such classification 'apriori' seem possible) the last determinant with the number genera greater or equal to 32 is -9240, and to it corresponds the classification XXXII, 2. Some idea of the growth of the number of classes is given in *Gauss's formula*

$$h(-1)+h(-2)+\ldots+h(-m)=\frac{4\pi}{21e}m^{\frac{3}{2}}-\frac{2}{\pi^2}m+m^{\frac{3}{4}}\rho_m \quad ** \qquad (1)$$

in which $h(-k)$ is the number of classes of properly primitive positive forms of determinant $-k$, symbol e denotes the sum of the series $1+1/2^3+1/3^3+\ldots$ and $|\rho_m|$ remains bounded for $m\to\infty$. Incidentally, Gauss has indicated only the first (leading) term of formula (1); in the form in which it is written here this formula has been given

* See Heilbronn, Q. J. Math. 1934. See also reference to Heegner and Stark on p. 239.

** I. M. Vinogradov improved this to $h(-1)+\ldots+h(-n)=4\pi n^{\frac{3}{2}}/21h(3)-2n/\pi+O(n^{t+\varepsilon})$ where $t=\frac{2}{3}$.

by I. M. Vinogradov. It follows from (1) that the arithmetical mean of n consequtive values of $h(-k)$, i.e. $(h(-k-1)+h(-k-2)+\ldots+h(-k-n))/n$ for constant k and $n \to \infty$ grows approximately as $(4\pi/21e)\sqrt{n}-e/\pi^2$.

For *positive* non-square determinants the number of classes has a smaller value than for negative; small classifications, as for example I, 1; II, 1, etc. are met here much more frequently and are continuous over the whole length of the table. For example, out of 90 nonsquare determinants occuring in the first hundred 11, 48 and 27 determinants have classifications I, 1; II, 1 and IV, 1 respectively; only four determinants, namely $+37$, $+34$, $+82$, $+79$ have other classifications: I, 3; II, 2; II, 2; II, 3. Out of 197 non-square determinant lying between 801 and 1000 (including the limits), 145 have one class in every genus.

Let K be a class of the principal genus of forms of determinant d and let $\alpha > 0$ be the least power for which $K^\alpha = 1$ (by composition); then α is a divisor of the number of classes h of the principal genus (§ 10, ch. IV). Determinant d is called *regular* (Gauss [20], D.A., art. 306), if there exists a class K for which $\alpha = h$, i.e. if all classes of the principal genus are the powers of one of them; otherwise d is called an *irregular* determinant. If α_0 is the greatest possible value of the power α and $\alpha_0 < h$, then the integer $h/\alpha_0 > 1$ is called the exponent *of irregularity*, of determinant d. Irregular determinants occur much less frequently than regular ones, for example, in the first thousand of negative determinants there are only 13 irregular, whose absolute values are

243,	307,	339,	459,	576,	580,	675,	755,	820,	884,	891,	900,	974
3	3	3	3	2	2	3	3	2	2	3	2	3

Under every determinant is written its exponent of irregularity. Similarly, in the second thousand there are 28 irregular determinants (13 with exponent 2 and 15 with exponent 3); in the third thousand the number of irregular determinants is 37, in the tenth thousand there are 63. Gauss (D.A. [20], art. 306) conjectured that the densities of distribution of regular and irregular negative determinants are in a definite ratio to each other, i.e. that the ratio M'/M'' (where M' and M'' are the numbers of regular and irregular determinants $d < 0$ for which $|d| \leqq m$) tend for $m \to \infty$ to a limit μ not equal to zero or

infinity; however, this proposition has not been proved by anyone. Among the positive non-square determinants the regular ones occur with much less frequency than among the negative ones.

Idoneal numbers of Euler, see notes to chapter II, p. 70, 71, are closely connected with the theory of quadratic forms; it is not difficult to see that the property of idoneal number mentioned there occurs when and only when in every genus of properly primitive order of determinant $-n$ there exists only one class of forms. In this case all classes of determinant $-n$ are ambiguous. In fact, in the 1st, 5th, 7th, 8th and 9th rows of the above table we find 65 idoneal numbers of Euler.

§ 2. The Kronecker relation between the numbers of classes

In 1857 Kronecker published eight remarkable recurrence relations for the number of classes of binary forms of a negative determinant which he obtained when considering certain modular equations in the theory of elliptic functions. Another proof of these relations, though also based on the theory of elliptic functions, but a simpler one than Kronecker's, was proposed by Hermite. Generalising the methods of Kronecker and Hermite, the other authors (Gierster, Klein, Hurwitz, Humbert) obtained a set of new formulae of the same type. Later there were found purely arithmetical ways of obtaining relations between the number of classes. First of all, Kronecker himself in his memoir 'Über bilineare Formen mit vier Variabeln' (see [35]) obtained some of his relations, by considering the equivalence of bilinear forms and defining the number of classes of such forms by means of two methods. Further, Liouville in his letter to Hermite has mentioned that relations which he was studying may be deduced from his numerical identities (§ 4, ch. 4), and described in general the outline of his reasoning. Finally, Uspensky [64] has given a complete proof of all relations of Kronecker, Gierster, Hurwitz, etc. by means of Liouville's methods. We use his exposition for the proof of the most important of Kronecker's relations.

Let n be a given integer. Denote by N the number of solutions*

* L. J. Morell. On the number of solutions in positive integers of the equation $yz+za+ay = n$. Am. J. Math. 45 (1923) 1–4. R. F. Whitehead. Same title. Proc. London Math. Soc. (2) 21, 1923.

of an indeterminate equation $4n+1 = d\delta+2d'\delta'$ in positive integers d, δ, d', δ' under the conditions $\frac{1}{2}(d+\delta) = d'+\varepsilon$, $\varepsilon = \pm 1$, δ' – odd. Thus, in the notations of the previous chapter

$$N = N\left(4n+1 = d\delta+2d'\delta', \frac{d+\delta}{2} = d'+\varepsilon, d, \delta, d', \delta' > 0, \delta' \text{ odd}\right) \tag{2}$$

Assuming for $\varepsilon = +1$ the odd integers d and δ to be equal to $2u+1$ and $2v+1$ ($u \geqq 0$, $v \geqq 0$) and taking $\delta' = 2k-1$ ($k > 0$) we obtain from equations $d'+1 = \frac{1}{2}(d+\delta)$, $4n+1 = d\delta+2d'\delta'$ the following equations

$$d' = u+v, \; n = uk+vk+uv, \; *$$

so that the number of solutions with $\varepsilon = +1$ may be represented in the form

$$N(n = uk+vk+uv, u \geqq 0, v \geqq 0, k > 0)$$
$$= N(n = uk+vk+uv, u, v, k > 0)+2N(n = d\delta, d, \delta > 0).$$

Similarly, taking for $\varepsilon = -1$

$$d = 2u-1, \delta = 2v-1, \delta' = 2k+1,$$

we find that the number of solutions with $\varepsilon = -1$ is equal to

$$N(n = uk+vk+uv, u, v > 0, k \geqq 0)$$
$$= N(n = uk+vk+uv, u, v, k > 0)+N(n = d\delta, d, \delta > 0).$$

so that for the total number N of solutions we obtain the following expression

$$N = 2N(n = uk+vk+uv, u, v, k > 0)+3N(n = d\delta, d, \delta > 0) \tag{3}$$

Since equation $n = uk+vk+uv$ is symmetric with respect to u, v, k the number of solutions of this equation, in which u, v, k have distinct positive values is six times the number of solutions in which $0 < k < u < v$; to every solution of the latter kind corresponds the form $(u+k, k, v+k) = (a, b, c)$ of determinant $-n$, for which $0 < 2b < a < c$. Further, to every solution u, v, k for which $0 < k < u = v$ there corresponds a form $(u+k, k, v+k) = (a, b, c)$ for which

* The formula for the number of solutions of $yz+zx+xy = u$ is due to Mordell 1923. See his Diophantine equations page 292 references given on page 218.

$0 < 2b < a$; finally to every solution for which $0 < u = v < k$, corresponds form $(u+v, k, u+k) = (2b, b, c)$ for which $2b < c$. Consequently,

$$N(n = uk+vk+uv, u, v, k > 0$$
$$= 6N(n = ac-b^2, 0 < 2b < a < c)+3N(n = a^2-b^2, 0 < 2b < a)$$
$$+3N(n = 2bc-b^2, 0 < 2b < c)+N(n = 3s^2, s > 0)$$

Noting also that $N(n = d\delta, d, \delta > 0) = 2N(n = ac, 0 < a < c) + N(n = s^2, s > 0)$ we obtain from (3)

$$N = 12N(n = ac-b^2, 0 < 2b < a < c)$$
$$+6N(n = a^2-b^2, 0 < 2b < a)+6N(n = 2bc-b^2, 0 < 2b < c)$$
$$+6N(n = ac, 0 < a < c)+2N(n = 3s^2, s > 0)+3N(n = s^2, s > 0) \quad (4)$$

On the other hand, denoting by $\bar{G}(n)$ the number of classes of positive forms of determinant $-n$ and remembering the conditions of reducibility of such forms (inequalities (8), § 3, ch. IV), we may write

$$\bar{G}(n) = 2N(n = ac-b^2, 0 < 2b < a < c)$$
$$+N(n = a^2-b^2, 0 < 2b < a)+N(n = 2bc-b^2, 0 < 2b < c)$$
$$+N(n = ac, 0 < a < c)+N(n = s^2, s > 0)+N(n = 3s^2, s > 0).$$

Comparing this with (4) we find $N = 6\bar{G}(n)-3N(n = s^2, s > 0)-4N(n = 3s^2, s > 0)$. We introduce now a numerical function $G(n)$ which differs from $\bar{G}(n)$ only in cases $n = s^2$ or $n = 3s^2$ (formula (60)) § 16, ch. IV). Then we obtain the final result

$$N = 6G(n). \quad (5)$$

Denote again by $\bar{F}(n)$ the number of those classes of determinant $-n$ in whose forms at least one of the outside coefficients is odd, and introduce by (60) § 16, ch. IV a numerical function $F(n)$ which differs from $\bar{F}(n)$ only in the case when n is an odd square; then, by a similar reasoning we obtain for every $n > 0$

$$N\left(4n+1 = d\delta+2d'\delta', \frac{d+\delta}{2} = d' \pm 1, d, \delta, d', \delta' \text{ odd} > 0\right)$$
$$= 4F(n). \quad (6)$$

We complete definitions of functions $F(n)$, $G(n)$ for argument 0, assuming $F(0) = 0$, $G(0) = -\frac{1}{12}$.

To begin the proof of Kronecker's relations, denote by $n > 0$ a given integer, by $\Phi(x)$ – a given even function and by d', δ' any pair of positive odd numbers, satisfying the condition $2d'\delta' < 4n+1$. Applying (40) § 4, ch. V to number $m = 4n+1-2d'\delta' \equiv 3 \pmod 4$ and to odd function $f(x) = \Phi(x-d')-\Phi(x+d')$ we obtain

$$\sum_{4n+1-2d'\delta' = 4h^2+d\delta} \left[\Phi\left(\frac{d+\delta}{2}-d'\right)-\Phi\left(\frac{d+\delta}{2}+d'\right)\right] \text{ [1])}$$
$$= 2 \sum_{4n+1-2d'\delta' = i^2+2d\delta} [\Phi(d-d'+i)-\Phi(d+d'+i)].$$

Adding these equalities for all pairs of positive odd numbers d', δ', satisfying, the condition $4n+1-2d'\delta' > 0$, we get

$$\sum_{4n+1=4h^2+d\delta+2d'\delta',\, d',\, \delta' \text{ odd}} \left[\Phi\left(\frac{d+\delta}{2}-d'\right)-\Phi\left(\frac{d+\delta}{2}+d'\right)\right] \tag{7}$$
$$= 2 \sum_{4n+1=i^2+2d\delta+2d'\delta',\, d,\, \delta,\, d',\, \delta' \text{ odd}} [\Phi(d-d'+i)-\Phi(d+d'+i)]$$

Since in the partition $4n+1 = i^2+2d\delta+2d'\delta'$ the number i may be greater or less than zero, the right hand side of (7) may be represented in the form

$$\sum_{4n+1=i^2+2d\delta+2d'\delta',\, \delta,\, d',\, \delta'} [\Phi(d-d'+i)-\Phi(d+d'+i)+\Phi(d-d'-i)$$
$$-\Phi(d+d'-i)].$$

Part of this sum corresponding to some constant value i may be represented in the form $\sum[\psi(d-d')-\psi(d+d')]$ where $\psi(x) = \Phi(x+i)$ $+\Phi(x-i)$ is an even function and the summation is performed over all representations $\frac{1}{2}(4n+1-i^2) = d\delta+d'\delta'$, d, δ, d', δ' odd > 0; applying (50) § 4, ch V, we obtain for this sum the expression

$$\sum_{\frac{1}{2}(4n+1-i^2)=d\delta,\, \delta \text{ odd}} d(\psi(0)-\psi(2d))$$

which enables us to represent the right hand side of (7) in the form

$$\sum_{4n+1=i^2+4d\delta,\, \delta \text{ odd}} 2d(\Phi(i)-\Phi(i-2d))$$
$$= \sum_{4n+1=i^2+2d\delta,\, \delta \text{ odd}} d(\Phi(i)-\Phi(i-d)).$$

Thus, (7) gives

---

[1]) See translator's notes to p. 166.

$$\sum_{4n+1=4h^2+d\delta+2d'\delta',\, d',\, \delta' \text{ odd}} \left[\Phi\left(\frac{d+\delta}{2}-d'\right)-\Phi\left(\frac{d+\delta}{2}+d'\right)\right]$$

$$= \sum_{4n+1=i^2+2d\delta,\, \delta \text{ odd}} d(\Phi(i)-\Phi(i-d)). \quad (8)$$

Assume in this identity $\Phi(x) = 0$ for $x^2 \neq 1$ and $\Phi(\pm 1) = 1$; such choice of the function does not contradict the condition that the function must be even Since $\frac{1}{2}(d+\delta)+d' > 1$, the left hand side of (8) with such choice of $\Phi(x)$ gives the number of solutions of an indeterminate equation $4n+1 = 4h^2+d\delta+2d'\delta'$ with respect to h, d, d', δ' satisfying the conditions $h \gtrless 0$, d, δ, d', δ' odd > 0, $\frac{1}{2}(d+\delta) = d' \pm 1$. Using formula (6), we find that this number of solutions is equal to the sum $4\sum F(n-h^2)$ taken over all $h = 0, \pm 1, \pm 2, \ldots$ for which $h^2 \leqq n$. The right hand side of (8) for a given choice of $\Phi(x)$ becomes $4\sum_{n=d\delta,\, \delta \text{ odd}} d - 2\sum_{n=d(d\pm 1+\delta)\, \delta \text{ odd}} d$. Denoting the factors d and $d \pm 1+\delta$ in the product $n = d(d\pm 1+\delta)$ by Δ and Δ' we can write

$$\sum_{n=d(d\pm 1+\delta),\, \delta \text{ odd}} d = \sum_{n=\Delta\Delta',\, \Delta<\Delta',\, \Delta+\Delta' \text{ even}} \Delta + \sum_{n=\Delta\Delta',\, \Delta\leqq\Delta',\, \Delta+\Delta' \text{ even}} \Delta$$

$$= 2 \sum_{n=\Delta\Delta',\, \Delta<\Delta',\, \Delta+\Delta' \text{ even}} \Delta + \sum_{n=s^2,\, s>0} \{s\}.$$

Collecting the above results together, we obtain from (8) the first recurrence relation for function $F(n)$

$$\sum_{h=0,\, \pm 1,\, \pm 2,\ldots,\, h^2\leqq n} F(n-h^2)$$

$$= \sum_{n=d\delta,\, \delta \text{ odd}} d - \sum_{n=\Delta\Delta',\, \Delta<\Delta',\, \Delta+\Delta' \text{ even}} \Delta - \frac{1}{2} \sum_{n=s^2,\, s>0} \{s\}. \quad (9)$$

To deduce the second relation, take again an integer $n > 0$ and an even function $\Phi(x)$; starting from (41) § 4, ch. V, we obtain, similarly to the above,

$$\sum_{4n+1=4h^2+d\delta+2d'\delta',\, d',\, \delta' \text{ odd}} (-1)^h \left[\Phi\left(\frac{d+\delta}{2}-d'\right)-\Phi\left(\frac{d+\delta}{2}+d'\right)\right]$$

$$= 2 \sum_{\substack{4n+1=i^2+2d\delta+2d'\delta' \\ d,\, \delta,\, d',\, \delta' \text{ odd}}} (-1)^{\frac{1}{2}(i-1)+\frac{1}{2}(\delta-1)}[\Phi(d-d'+i)-\Phi(d+d'+i)].$$

The right hand side here is simplified by means of (51) § 4, ch. V after which the equality becomes

$$\sum_{4n+1=4h^2+d\delta+2d'\delta',\ d'\delta' \text{ odd}} (-1)^h \left[\Phi\left(\frac{d+\delta}{2}-d'\right)-\Phi\left(\frac{d+\delta}{2}+d'\right)\right]$$
$$= 2 \sum_{4n+1=i^2+4d\delta,\ \delta \text{ odd}} (-1)^{\frac{1}{2}(i-1)+\frac{1}{2}(\delta-1)} d\Phi(i-2d).$$

Taking here again $\Phi(x) = 0$ for $x \neq \pm 1$ and $\Phi(\pm 1) = 1$ we obtain after simple transformations, the second recurrence relation for $F(n)$

$$\sum_{h=0,\ \pm 1,\ \pm 2,\ldots,\ h^2 \leqq n} (-1)^h F(n-h^2)$$
$$= \sum_{n=\Delta\Delta',\ \Delta<\Delta',\ \Delta+\Delta' \text{ even}} (-1)^{\frac{1}{2}(\Delta+\Delta')+1}\Delta + \frac{1}{2}\{(-1)^{s-1}s\}. \quad (10)$$
$$n=s^2,\ s>0$$

Starting from formula (40) § 4, ch. V we obtain for a given number n and even function $\Phi(x)$

$$\sum_{4n+1=4h^2+d\delta+2d'\delta',\ \delta' \text{ odd}} \left[\Phi\left(\frac{d+\delta}{2}-d'\right)-\Phi\left(\frac{d+\delta}{2}+d'\right)\right]$$
$$= 2 \sum_{4n+1=i^2+2d\delta+2d'\delta',\ \delta,\ \delta' \text{ odd}} [\Phi(d-d'+i)-\Phi(d+d'+i)]$$
$$+ \sum_{4n+1=i^2+2d\delta,\ \delta \text{ odd}} i\Phi(i-d).$$

The first sum in the right hand side is simplified by means of (48) § 4, ch. V, and the equality becomes

$$\sum_{4n+1=4h^2+d\delta+2d'\delta',\ \delta' \text{ odd}} \left[\Phi\left(\frac{d+\delta}{2}-d'\right)-\Phi\left(\frac{d+\delta}{2}+d'\right)\right]$$
$$= 2 \sum_{4n+1=i^2+2d\delta,\ \delta \text{ odd}} (\delta-d)[\Phi(d+i)-\Phi(i)] + \sum_{4n+1=i^2+2d\delta,\ \delta \text{ odd}} i\Phi(i-d).$$

Taking here $\Phi(x) = 0$ for $x \neq \pm 1$ and $\Phi(\pm 1) = 1$ and using (5) we find

$$3 \sum_{h=0,\ \pm 1,\ \pm 2,\ldots,\ h^2 \leqq n} G(n-h^2)$$
$$= 2 \sum_{n=\Delta\Delta',\ \Delta<\Delta',\ \Delta+\Delta' \text{ even}} (\Delta'-2\Delta) + 2\zeta(n) - \{s\} \quad (11)$$
$$n=s^2,\ s>0$$

where $\zeta(n)$ denotes, as usual, the sum of the divisors of n. Similarly, we deduce the relation

$$3 \sum_{h=0,\ \pm 1,\ \pm 2,\ldots,\ h^2 \leqq n} (-1)^h G(n-h^2)$$
$$= \sum_{n=\Delta\Delta',\ \Delta<\Delta',\ \Delta+\Delta' \text{ even}} (-1)^{\frac{1}{2}(\Delta+\Delta')}(\Delta'-5\Delta) + 2\{(-1)^{s-1}s\}. \quad (12)$$
$$n=s^2,\ s>0$$

Relations (9) and (11) together with the Jacobi theorem on the number of representations as a sum of four squares (theorem 23 § 5, ch. V) allow us to prove again Gauss's theorem on the number of representations by three squares (theorem 18, or equality (67) § 16, ch. IV). Namely, from (9) and (11), by means of simple operations, we deduce

$$3\sum_{h^2\leqq n}[2F(n-h^2)-G(n-h^2)] = 2(2+(-1)^n)\sum_{n=d\delta,\ \delta\ \text{odd}}\delta$$

On the other hand, denoting by $N_3(n)$ the number of representations of n as a sum of three squares, so that $N_3(0) = 1$, we can write by the Jacobi theorem,

$$\sum_{h^2\leqq n} N_3(n-h^2) = 8(2+(-1)^n)\sum_{n=d\delta,\ \delta\ \text{odd}}\delta$$

comparing this with the previous equality we obtain

$$\sum N_3(n-h^2) = 12\sum[2F(n-h^2)-G(n-h^2)],$$

from which, by induction, we obtain for every n

$$N_3(n) = 12(2F(n)-G(n)) \tag{13}$$

i.e. formula (67) § 16, ch. IV. Adding formulae (9) and (10), replacing in the obtained formula n by $4n$ and comparing the result with (9), we find

$$\sum_{h^2\leqq n} F(4n-4h^2) = 2\sum_{h^2\leqq n} F(n-h^2)$$

from which, for every n, we deduce $F(4n) = 2F(n)$. This property of the function $F(n)$ has been proved in § 16, ch. IV (formula (66)) by means of the Gaussian theory of quadratic forms. Further, denote by m any odd number; since in equation $4m = x^2+y^2+z^2+t^2$ all numbers x, y, z, t are simultaneously even or odd, we may write by Jacobi's theorem 23

$$N(4m = x^2+y^2+z^2+t^2,\ x\ \text{odd}) = \sum_{x=\pm1,\pm3,\ldots} N_3(4m-x^2) = 16\zeta(m).$$

On the other hand, subtracting from (9) formula (10) and assuming in the obtained equality $n = 4n$, we find

$$\sum_{x=\pm1,\pm3,\ldots} F(4m-x^2) = 2\zeta(m),$$

comparing this with the previous equality gives

$$\sum N_3(4m-x^2) = 8\sum F(4m-x^2),$$

from which for every $n \equiv 3 \pmod 8$ we deduce $N_3(n) = 8F(n)$. Comparing this with (13) we obtain for $n \equiv 3 \pmod 8$

$$G(n) = \tfrac{4}{3}F(n)$$

Similarly we may prove all the remaining relations between functions $F(n)$ and $G(n)$, listed in § 16, ch. IV (formulae (62), (64) and (66)).

From the result we have just obtained, we deduce one more necessary formula. Taking $m \equiv 7 \pmod 8$ consider the sum

$$S = \sum_{h=0,\,\pm1,\,\pm2,\ldots} F(m-16h^2);$$

clearly

$$S = \sum_{h=0,\,\pm1,\ldots} F(m-4h^2) - \sum_{i=\pm1,\,\pm3,\ldots} F(m-4i^2).$$

For the first sum, on adding (9) and (10), we find the expression

$$\sum F(m-4h^2) = \tfrac{1}{2}\zeta(m) - \sum_{m=\Delta\Delta',\,\Delta<\Delta'} \Delta. \tag{14}$$

In the second sum $\sum F(m-4i^2)$ all the arguments of function $F(n)$ are of the form $8k+3$; therefore, using the result just proven: $N_3(8k+3) = 8F(8k+3)$, we can write

$$\sum F(m-4i^2) = \tfrac{1}{8}N(m = x^2+y^2+z^2+4i^2,\ i \text{ odd})$$

Noting that for $m \equiv 7 \pmod 8$ in equation $m = x^2+y^2+z^2+t^2$ among the numbers x, y, z, t three are always odd, and the fourth is twice an odd number, we obtain, by the Jacobi theorem

$$\sum F(m-4i^2) = \tfrac{1}{4}\zeta(m).$$

This result together with (14) finally gives

$$\sum_{h=0,\,\pm1,\,\pm2,\ldots} F(m-16h^2) = \tfrac{1}{4}\sum_{m=\Delta\Delta',\,\Delta<\Delta'} (\Delta'-3\Delta), \quad m \equiv 7 \pmod 8. \tag{15}$$

Starting from formula (40) § 4, ch. V, we obtain for n an integer, and $\Phi(x)$ an even function

$$\sum_{2n=4h^2+d\delta+d'\delta',\ d,\ \delta,\ d',\ \delta'\ \text{odd}} [\Phi(d+\delta-d')-\Phi(d+\delta+d')]$$

$$= 2 \sum_{\substack{2n=i^2+d\delta+2d'\delta' \\ d,\ \delta,\ \delta'\ \text{odd}}} [\Phi(2d'-d+2i)-\Phi(2d'+d+2i)]+\sum_{\substack{2n=i^2+d\delta \\ i\ \text{odd}}} i\Phi(2i-d).$$

Simplifying the first sum on the right hand side by means of identity (53) § 4, ch. V, we obtain

$$\sum_{n=4h^2+d\delta+d'\delta',\ d,\ \delta,\ d',\ \delta'\ \text{odd}} [\Phi(d+\delta-d')-\Phi(d+\delta+d')]$$

$$= \sum_{2n=i^2+d\delta,\ i\ \text{odd}} (\delta-d+i)\Phi(2i-d).$$

Assuming here, as usual $\Phi(\pm 1) = 1$ and $\Phi(x) = 0$ for the remaining values of x, we obtain

$$\sum_{h=0,\ \pm 1,\ \pm 2,\ \ldots,\ 2h^2<n} \psi(n-2h^2) = \tfrac{1}{4} \sum_{8n-1=\Delta\Delta',\ \Delta<\Delta'} (\Delta'-3\Delta),$$

where $\psi(n)$ denotes the number of solutions of equation $2n = d\delta+d'\delta'$ in positive odd integers d, δ, d', δ' satisfying the condition $d+\delta = d'\pm 1$. Comparing the obtained equality with (15) gives

$$\sum \psi(n-2h^2) = \sum F(8n-16h^2-1)$$

from which for every n $\psi(n) = F(8n-1)$, i.e.

$$N(2n = d\delta+d'\delta',\ d+\delta = d'\pm 1,\ d,\ \delta,\ d',\ \delta'\ \text{odd}\ > 0) = F(8n-1). \quad (16)$$

This result could also be deduced directly using a reasoning similar to the one at the beginning of this section. Finally using first (41) and then (54) § 4, ch. V, we obtain equality

$$\sum_{2n=4h^2+d\delta+d'\delta',\ d,\ \delta,\ d',\ \delta'\ \text{odd}\ >0} (-1)^h[\Phi(d+\delta-d')-\Phi(d+\delta+d')]$$

$$= \sum_{2n=i^2+d\delta,\ i\ \text{odd}} (-1)^{\frac{1}{2}(i-1)+\frac{1}{2}(\delta-1)} d\Phi(d-2i).$$

Taking in it $\Phi(x) = 0$ for $x \neq \pm 1$ and $\Phi(\pm 1) = 1$ and using (16) we find

$$\sum_{h=0,\ \pm 1,\ \pm 2,\ \ldots} (-1)^h F(m-16h^2) = -\sum_{m=\Delta\Delta',\ \Delta<\Delta'} (-1)^{\frac{1}{2}(\Delta+\Delta')}\Delta \quad (17)$$

$$m \equiv 1 \pmod 8.$$

The relations (9), (10), (11), and (17) deduced here are equivalent to the first seven relations of Kronecker; his eighth relation has a more complicated form

$$\sum (-1)^{(m-i^2)/16}\left[2F\left(\frac{m-i^2}{16}\right)-3G\left(\frac{m-i^2}{16}\right)\right] = \sum_{m=\Delta\Delta',\ \Delta<\Delta'} (-1)^{\frac{1}{2}(\Delta'-\Delta)}\Delta + \sum_{m=s^2,\ s>0}\{\tfrac{1}{2}s\}, \quad m\equiv 1 (\mathrm{mod}\ 8), \quad (18)$$

where on the left hand side the summation is performed over all odd $i=\pm 1, \pm 3, \pm 5, \ldots$ for which $i^2 \leqq m$ and $(m-i^2)/16$ is an integer. The proof of this formula may be found in Uspensky's [64] memoir referred to above (Premier Mem., II, § 12).

Kronecker applied his relations to the solution of the problem mentioned in § 5, ch. I, i.e. to deduce a practical convenient rule for the definition of the sign $\pm$ in congruence $(\frac{1}{2}(p-1))! \equiv \pm 1 \pmod p$ for a prime p of the form $4n+3$. It has already been shown in § 5, ch. I that $(\frac{1}{2}(p-1))! \equiv (-1)^{\beta} \pmod p$ where $\beta = \frac{1}{4}(p-1)-\frac{1}{2}h$ and $h = F(p)$ is the number of properly primitive forms of determinant $-p$. From relations (9) and (10) we find the following expression for β:

$$\beta = F(p-4\cdot 1^2)+F(p-4\cdot 2^2)+F(p-4\cdot 3^2)+\ldots \quad (19)$$

To determine the parity of this number it remains to solve the following problem: for which arguments $n \equiv 3 \pmod 4$ is the value of $F(n)$ even, and for which odd? For this, using the conditions for positive forms to be reduced (inequalities (8) § 3, ch. IV), we write expression

$$F(n) = 2N(n = ac-b^2,\ 0<2b<a<c,\ a \text{ or } c \text{ odd})+ \\ +N(n=ac,\ 0<a<c,\ a \text{ or } c \text{ odd},$$

where on the right hand side we omitted the reduced forms of the form (a, b, a) and $(2b, b, c)$, since their outside coefficients for $n \equiv 3 \pmod 4$ are even. From here we obtain congruence $F(n) \equiv \frac{1}{2}\tau(n) \pmod 2$ where $\tau(n)$ is the number of divisors of n. Taking into account the known expression for $\tau(n)$ (§ 2, ch. I), we find that for $n \equiv 3 \pmod 4$ $F(n)$ is odd if and only if the argument n is of the form $q^{4k+1}s^2$ where q is a prime (clearly, of the form $4l+3$) combining this together with formula (19), we finally obtain the following Kronecker criterion: *for a prime* $p \equiv 3 \pmod 4$ *in congruence*

$(\frac{1}{2}(p-1))! \equiv \pm 1 \pmod{p}$, *the sign is* + *or* − *according as the number of representations of* p *in the form* $4h^2+q^{4k+1}s^2$ (*where* $h>0$, $s>0$, $k \geqq 0$ *are integers, and* q *is a prime*) *is even or odd.*

§ 3. The Dirichlet formulae

Dirichlet in his memoir 'Recherches sur diverses applications de l'analyse infinitésimale à la théorie des nombres' (1839) published remarkable expressions for the number of classes of binary forms of positive and negative determinant, which are now called the Dirichlet formulae; these expressions were obtained by him in considering certain infinite series; these expressions were already known to Gauss, which is indicated in the fragments of his posthumous manuscripts published in volume II of his collected works. ('De nexu inter multitudinem classium, in quas formae binaire secundi gradus distribuuntur earumque determinantem' see also [20], p. 655–677).

Let $d = \pm m$ be an integer without a squared factor, and let $h(\pm m)$ be the number of primitive classes of forms of determinant d, positive for $\pm m < 0$.

We select one form from each such class K say, $a_ix^2+2b_ixy+c_iy^2$, $(a_i>0)$ and assume a real parameter $s>1$. According to the theorem proved in the end of § 8, ch. IV, we can write the identity

$$\sum_K \zeta(K,s) = \varkappa \sum_m \frac{1}{m^s} \sum_{m=\Delta\Delta',\, \Delta \text{ odd}} \left(\frac{d}{\Delta}\right), \qquad (*)$$

where

$$\zeta(K,s) = \sum_{x,y} \frac{1}{(a_ix^2+2b_ixy+c_iy^2)^s}.$$

In the left hand side of this identity the summation is performed over all properly primitive classes K of determinant d; and in every sum $\zeta(K,s)$ the numbers x, y run through all pairs of integers, not simultaneously zero, for which $a_ix^2+2b_ixy+c_iy^2$ is relatively prime to $2d$ and which satisfy inequalities $y \geqq 0$, $U(a_ix+b_iy) > Ty$ for $d=m>0$ (T, U – the smallest solution of equation $t^2-mu^2=1$). In the right hand side of (*) the sum is taken over all $m>0$ relatively prime to $2d$ and, for every m, over all odd divisors Δ of m. The factor $\varkappa$ (§ 8, ch. IV) is equal to 1 for $d>0$ and to 2 for $d<-1$. Multi-

plying the identity (*) by $s-1$ and passing over to limits as $s \to 1$, Dirichlet obtains the required expressions for the number of classes. The right hand side of (*) becomes the product of two series $\varkappa \sum 1/\Delta^s$ and $\sum (d/\Delta) 1/\Delta^s$ (in which the summation is performed over all $\Delta > 0$, relatively prime to $2d$); it is not difficult to prove that

$$\lim_{s \to 1} (s-1) \sum \frac{1}{\Delta^s} = \frac{\varphi(2m)}{2m}, \quad \lim_{s \to 1} \sum \left(\frac{d}{\Delta}\right) \frac{1}{\Delta^s} = \sum \left(\frac{d}{\Delta}\right) \frac{1}{\Delta}.$$

In the left hand side of (*) we first evaluate the limit of $(s-1)\zeta(K, s)$ as $s \to 1$ for a single class K. By means of ingenious lemmas (see L. Dirichlet [14], Suppl. III and IX) the evaluation of this limit is reduced to the evaluation of the area of the ellipse $a_i x^2 + 2b_i xy + c_i y^2 \leqq 1$ for $d < 0$, or the area of a hyperbolic sector $a_i x^2 + 2b_i xy + c_i y^2 \leqq 1$, $y \geqq 0$, $U(a_i x + b_i y) > Ty$ for $d > 0$. This provides for $\lim_{s \to 1} (s-1)\zeta(K, s)$ a value $(\varphi(2m)/2m)\lambda$ independent of K, where

$$\lambda = \frac{\pi}{\sqrt{m}} \qquad \text{for } d = -m < 0$$

and

$$\lambda = \frac{1}{2\sqrt{m}} \log (T + U\sqrt{m}) \qquad \text{for } d = m > 0.$$

Identity (*) then gives

$$h(d) = \frac{\varkappa}{\lambda} \sum_{\Delta} \left(\frac{d}{\Delta}\right) \frac{1}{\Delta}.$$

The series on the right hand side (not absolutely convergent) belongs to the series summable by means of definite integrals. The reader who is interested in a detailed proof is referred to the textbook by Dirichlet [14]; we produce here only the final result. Namely, for $d = -m < -1$ we obtain

$$h(-m) = \sum \left(\frac{-m}{a}\right), \tag{20}$$

$$0 < a < m, \quad (a, 2m) = 1, \quad m \equiv 1, 2 \pmod 4$$

$$h(-m) = \sum \left(\frac{b}{m}\right), \tag{21}$$

$$0 < b < \tfrac{1}{2}m, \quad (b, m) = 1, \quad m \equiv 3 \pmod 4$$

where the summation is performed over all integers a, b satisfying the conditions written underneath the sums. For a positive determinant the Dirichlet formulae are of the form

$$h(m) = -\frac{2-\left(\frac{2}{m}\right)}{\log(T+U\sqrt{m})}\sum\left(\frac{b}{m}\right)\log\sin\frac{\pi b}{m} \tag{22}$$

$$0 < b < m, \quad (b, m) = 1, \quad m \equiv 1 \pmod 4$$

$$h(m) = -\frac{1}{\log(T+U\sqrt{m})}\sum\left(\frac{m}{a}\right)\log\sin\frac{\pi a}{4m} \tag{23}$$

$$0 < a < 4m, \quad (a, 2m) = 1, \quad m \equiv 2, 3 \pmod 4$$

A partial purely arithmetical proof of Dirichlet's formulae for negative determinant (namely the proof of formula (20)) is given in the next section.

Let us note one important case of formula (21): for m equal to a prime p this formula shows that *the number of classes of properly primitive binary forms of determinant* $-p$ (p *is a prime of the form* $4k+3$) *is equal to the difference between the number of quadratic residues and quadratic non-residues modulo* p *among the numbers* $1, 2, \ldots, \frac{1}{2}(p-1)$.

Since $h(-p)$ is always greater than zero, it follows that among the numbers $1, 2, \ldots, \frac{1}{2}(p-1)$ there are more quadratic residues than quadratic non-residues. In spite of simplicity of this fact there is as yet no elementary proof of it. The formulated proposition enables us to find an estimate for the value of $h(-p)$ namely, applying the theorem of I. M. Vinogradov on the number of quadratic residues in a progression (§ 2, ch. III), we obtain an inequality of the form $h(-p) < c\sqrt{p}\log p$ where c is a constant. A similar inequality may be obtained for $(h-m)$ and for m which is square free.

§ 4. Proof of the Dirichlet formulae for the properly primitive case of a negative determinant

The author of the present monograph has shown in 1927 (see B. A. Venkov [96]), that starting from Gauss's theorems on the representation of numbers and binary forms by three squares (§ 16,

ch. IV), we may give purely arithmetical proof of Dirichlet's formulae for all negative determinants $-m$ in which m is the sum of three squares, i.e. for $m \equiv 1$ or $m \equiv 2 \pmod 4$ and $m \equiv 3 \pmod 8$ (see § 16, ch. IV). In the present section we give this proof, restricting ourselves to the simpler case $m \equiv 1, 2 \pmod 4$. First of all, consider the concluding theorem § 16, ch. IV, giving the number of representations of a positive binary form $kx^2+2lxy+k'y^2$ (in which k is square free) as a sum of three squares. Taking all factorisations of number $kk'-l^2 = d\delta$ into two factors $d > 0$, $\delta > 0$ in which δ is odd and k, d, δ have no common factor, let us assume for each factorisation $(k, \delta) = \Delta, k = \Delta\bar{k}$ and consider the sum $S_l = 24 \sum (-1)^{\frac{1}{2}(\Delta-1)\cdot\frac{1}{2}(\delta-1)} (-d/\Delta)(-\bar{k}/\delta)$ taken over all such factorisations. Remembering the definition of the numbers p, q, P, Q, N introduced in the proof of theorem § 16, ch. IV (formula (69)) we may say that every power p^α, q^β enters into only one factor d, δ. Thus, denoting the greatest common divisors of d, δ with each number P, Q, N, L by the table

	P	Q	N	L
d	r	t	v	d_0
δ	s	u	w	δ_0

we may write

$$P = rs, \quad Q = tu, \quad N = vw, \quad L = d_0\delta_0, \quad \Delta = suw,$$

$$\bar{k} = \frac{PQNR}{suw} = rtvR.$$

Conversely, the numbers $r, s, \ldots, d_0, \delta_0$ determine completely the decomposition of $kk'-l^2$ into factors d, δ satisfying the posed conditions. Thus, summation in expression S_l is performed if we take the numbers s, u, w, δ_0 run, independently of each other, through all odd divisors of coprime numbers P, Q, N, L respectively (§ 16, ch. IV) Since each number d, δ differs by a square from tvd_0 and $uw\delta_0$, the expression under the summation sign of S_l may be represented in the form

$$(-1)^{\frac{1}{2}(\Delta-1)\cdot\frac{1}{2}(uw\delta_0-1)} \left(\frac{-tvd_0}{\Delta}\right)\left(\frac{-\bar{k}}{uw\delta_0}\right)$$

or, on simplification, in the form

$$\left(\frac{-QNL}{s}\right)\left(\frac{-PRL}{uw}\right)\left(\frac{-k}{\delta_0}\right).$$

Taking into account the fact that numbers P, Q, N are square free, we obtain the following expression for S_l:

$$S_l = 24\prod\left[1+\left(\frac{-QNL}{p}\right)\right] \times \prod\left[1+\left(\frac{-PRL}{q}\right)\right]\cdot\prod\left[1+\left(\frac{-PRL}{n}\right)\right]\sum\left(\frac{-k}{\delta_0}\right) \quad (24)$$

where the first product is taken over all odd primes p, the second – over all odd primes q, the third – over all odd divisors n of the number N, and in the last sum over all odd divisors δ_0 of L. Formula (24) shows that if the conditions of the theorem § 16, ch. IV are satisfied, then the sum S_l is equal to the number of representations of $kx^2+2lxy+k'y^2$ as a sum of three squares (formula (71) § 16, ch. IV), if the conditions of the theorem are not satisfied, then $S_l = 0$. Thus, denoting as usual by N the number of representations we have in all cases

$$N(kx^2+2lxy+k'y^2 = (ax+a'y)^2+(bx+b'y)^2+(cx+c'y)^2) = S_l = 24\sum(-1)^{\frac{1}{2}(\Delta-1)\cdot\frac{1}{2}(\delta-1)}\left(\frac{-d}{\Delta}\right)\left(\frac{-k}{\delta}\right). \quad (25)$$

The last formula has the advantage over formula (71) § 16, ch. IV in the sense that it does not need preliminary listing of conditions of representability of $kx^2+2lxy+k'y^2$ as a sum of three squares.

Now, let $m > 1$ be an integer of the form either $4e+1$ or $4e+2$ not divisible by a square (i.e. the number for which we wish to prove Dirichlet's formula (20)). Assume in (25) $k = k' = m$ and noting that in this formula $|l| < m$, consider the sums $\sigma = \sum_{l\equiv m(\mathrm{mod}\ 2)} S_l$, $\sigma' = \sum_{l\equiv m+1(\mathrm{mod}\ 2)} S_l$ taken over all $l = 0, \pm1, \pm2, \ldots, |l| < m$ satisfying conditions for residues modulo 2 written under the summation sign. Using the *left* expression for S_l in (25) we may say that the sum σ is the number of systems of integers a, b, c, a', b', c' satisfying equations $m = a^2+b^2+c^2 = a'^2+b'^2+c'^2$ and additional

conditions $l = aa' + bb' + cc' \equiv m \pmod 2$, $|l| < m$. But from identity

$$(a^2+b^2+c^2)(a'^2+b'^2+c'^2) = (aa'+bb'+cc')^2+(bc'-cb')^2 + (ca'-ac')^2+(ab'-ba')^2$$

it follows that for every system of numbers a, b, c, a', b', c' satisfying equations $m = a^2+b^2+c^2 = a'^2+b'^2+c'^2$ we have $|aa'+bb'+cc'| \leqq m$ where equality $aa'+bb'+cc' = \pm m$ exists if and only if $a' = \varepsilon a$, $b' = \varepsilon b$, $c' = \varepsilon c$, $\varepsilon = \pm 1$. Now, using Gauss's theorem on the number of representations of m by three squares (theorem 18 § 16, ch. IV), and noting that for $m \equiv 1, 2 \pmod 4$ in equation $m = a^2+b^2+c^2$ one of numbers a, b, c is always congruent to m, and the remaining two $\equiv m+1 \pmod 2$ we can easily find for sum the expression

$$\sigma = 3(4h)^2 - 2 \cdot 12h = 24(2h^2-h),$$

where h is written in short for $h(-m)$. For the second sum we similarly find the expression $\sigma' = 24 \cdot 4h^2$. Taking into account the expressions obtained for sums σ, σ' and now using the *right* expression for S_l in (25) we obtain the following equalities

$$4h^2 = \sum (-1)^{\frac{1}{2}(\Delta-1)\cdot\frac{1}{2}(\delta-1)} \left(\frac{-d}{\Delta}\right)\left(\frac{-\overline{m}}{\delta}\right), \quad l \equiv m+1 \pmod 2, \quad (26)$$

$$2h^2 - h = \sum (-1)^{\frac{1}{2}(\Delta-1)\cdot\frac{1}{2}(\delta-1)} \left(\frac{-d}{\Delta}\right)\left(\frac{-\overline{m}}{\delta}\right), \quad l \equiv m \pmod 2. \quad (27)$$

On the right hand sides of these equalities the sums are extended over all solutions of equation $m^2 = l^2 + d\delta$ in integers l, d, δ satisfying the conditions $l \lesseqgtr 0$, $d > 0$, $\delta > 0$, δ odd, d, l, δ are coprime; moreover, l satisfies also congruences modulo 2 stated in the equalities (26), (27). Further, every system of numbers d, l, δ satisfies $(m, \delta) = \Delta$ and $m = \Delta\overline{m}$. Equalities (26) and (27) serve as the basis for further deductions.

To every representation $m^2 = l^2 + d\delta$ described above there corresponds a properly primitive binary form $(d, l, -\delta)$ of a positive square determinant m^2. Using the reduction of these forms (§ 6, ch. IV) we may say that the form $(d, l, -\delta)$ is equivalent to the form $(a, -m, 0)$ where $0 < a < 2m$ and $(a, 2m) = 1$. Denoting by $\begin{pmatrix} \xi & \eta \\ \zeta & \theta \end{pmatrix}$ the substitution, transforming $(a, -m, 0)$ into $(d, l, -\delta)$ (where we may assume $\xi > 0$ since the signs of ξ, η, ζ, θ may be simultaneously

changed), we have

$$d = a\xi^2 - 2m\xi\zeta, \quad \delta = 2m\eta\theta - a\eta^2, \quad \xi\theta - \eta\zeta = 1 \tag{28}$$

Moreover, from the theorem formulated at the end of § 6, ch. IV it follows that if the numbers d, l, δ are uniquely defined then a is defined in the form $(a, -m, 0)$, and the numbers ξ, η, ζ, θ are defined. From (28) and $d > 0, \delta > 0$, we obtain inequalities $\zeta/\xi < a/2m < \theta/\eta$. Since $\theta/\eta - \zeta/\xi = 1/\xi\eta > 0$ and since by supposition $\xi > 0$, we have $\eta > 0$. The condition that δ is odd is equivalent to the following: η odd. Finally, from $m^2 = l^2 + d\delta$ it follows that

$$l + m \equiv d\delta \equiv d \equiv \xi \pmod 2,$$

so that the congruences for l stated in equalities (26) and (27) are equivalent to the following: $\xi \equiv 1$ and $\xi \equiv 0 \pmod 2$. Taking into account the fact that $m \equiv 1, 2 \pmod 4$ we obtain, after a short calculation

$$(-1)^{\frac{1}{2}(\Delta-1)\cdot\frac{1}{2}(\delta-1)}\left(\frac{-d}{\Delta}\right)\left(\frac{-\overline{m}}{\delta}\right) = (-1)^{\theta+1}\left(\frac{-m}{a}\right).$$

Therefore, the summation in the right hand sides of (26) and (27) may be performed as follows: we perform the summation over all numbers $a > 0$ and $a < 2m$ relatively prime to $2m$ and, for every a, for all pairs of fractions ζ/ξ, θ/η satisfying conditions $\xi > 0$, $\eta > 0$, $\zeta/\xi < a/2m < \theta/\eta$, $\xi\theta - \eta\xi = 1$, η odd, and also the condition that ξ is odd for (26) and ξ is even for (27): the number of such pairs of fractions ζ/ξ, θ/η for a fixed a is finite, since by a known proposition (§ 1, ch. II) the denominators ξ, η do not exceed $2m$. Introduce for *rational* argument r arithmetical functions $\psi(r)$, $\psi'(r)$, $\psi''(r)$ by formulae

$$\psi(r) = \sum_{\xi,\,\eta\ \text{odd}} (-1)^{\zeta}, \quad \psi'(r) = \sum_{\xi\ \text{even}} (-1)^{\theta+1}, \quad \psi''(r) = \sum_{\eta\ \text{even}} (-1)^{\zeta} \tag{29}$$

where the summation is performed over all pairs of fractions ζ/ξ, θ/η satisfying the conditions

$$\zeta > 0, \quad \eta > 0, \quad \frac{\zeta}{\xi} < r < \frac{\theta}{\eta}, \quad \zeta\theta - \eta\zeta = 1 \tag{30}$$

and also the conditions written below every sum, then (26) and (27)

become:

$$4h^2 = \sum \left(\frac{-m}{a}\right) \psi\left(\frac{a}{2m}\right), \quad 2h^2 - h = \sum \left(\frac{-m}{a}\right) \psi\left(\frac{a}{2m}\right) \tag{31}$$

where the sums are taken over all a between 0 and $2m$ which are relatively prime to $2m$. To every pair of fractions ζ/ξ, θ/η satisfying conditions (30) there corresponds a pair of fractions $\zeta'/\xi' = (\eta-\theta)/\eta$, $\theta'/\eta' = (\xi-\zeta)/\xi$ for which $\xi' > 0$, $\eta' > 0$, $\zeta'/\xi' < 1-r < \theta'/\eta'$, $\xi'\theta' - \eta'\zeta' = 1$; from here it is easy to deduce the relations $\psi(1-r) = \psi(r)$, $\psi'(1-r) = \psi''(r)$. Noting also that for two positive numbers a, a' whose sum is $2m$ we have $(-m/a) = (-m/a')$ we obtain from (31) another formula

$$2h^2 - h = \sum \left(\frac{-m}{a}\right) \psi''\left(\frac{a}{2m}\right),$$

which together with (31) finally gives

$$h = \sum \left(\frac{-m}{a}\right) \left\{\psi\left(\frac{a}{2m}\right) - \psi'\left(\frac{a}{2m}\right) - \psi''\left(\frac{a}{2m}\right)\right\}. \tag{32}$$

Here, the summation is performed over all a between 0, m which are relatively prime to $2m$. To obtain the expression for numerical function

$$\psi\left(\frac{a}{2m}\right) - \psi'\left(\frac{a}{2m}\right) - \psi''\left(\frac{a}{2m}\right),$$

which enters formula (32), let us prove one lemma from the theory of continued fractions. Let $p > q \geqq 1$ be odd relatively prime numbers; consider the sums

$$\varphi\left(\frac{p}{q}\right) = \sum_{\alpha+\gamma,\, \beta+\delta \text{ odd}} (-1)^{\gamma}, \quad \varphi'\left(\frac{p}{q}\right) = \sum_{\beta,\, \delta \text{ odd}} (-1)^{\gamma}$$

$$\varphi''\left(\frac{p}{q}\right) = \sum_{\alpha,\, \gamma \text{ odd}} (-1)^{\beta} \tag{33}$$

taken over all pairs of fractions γ/α, δ/β satisfying the conditions

$$\alpha > 0, \quad \beta > 0, \quad \frac{\gamma}{\alpha} < \frac{p}{q} < \frac{\delta}{\beta}, \quad \alpha\delta - \beta\gamma = 1. \tag{34}$$

For $q = 1$ there are no such fractions (since we must have $1 > \alpha$,

$1 > \beta$) and, consequently, all sums (33) are zeros; if $q > 1$, then we find an even number $k \geqq 2$ and unit $\varepsilon = \pm 1$ such that $p = kq + \varepsilon r$ and $q > r \geqq 1$ where $(r, 2q) = 1$. First, let $\varepsilon = +1$, then $k < p/q < \delta/\beta$, consequently, $k \leqq \gamma/\alpha$ (since otherwise fraction $k/1$ lies between γ/α and δ/β). If $k < \gamma/\alpha$ the fraction q/r lies between fractions $\gamma'/\alpha' = \beta/(\delta - k\beta')$, $\delta'/\beta' = \alpha/(\gamma - k\alpha')$ which satisfy all other conditions (34); if $k = \gamma/\alpha'$, then $\alpha = 1$, $\gamma = k$, $\delta = k\beta + 1$, $0 < \beta < q/r$. Taking this into account, we obtain the following relations for $\varepsilon = +1$:

$$\varphi\left(\frac{p}{q}\right) = \left[\frac{q}{2r}\right] + \varphi\left(\frac{q}{r}\right),$$

$$\varphi'\left(\frac{p}{q}\right) = \left[\frac{q}{2r} + \frac{1}{2}\right] - \langle r\rangle + \varphi''\left(\frac{q}{r}\right), \quad \varphi''\left(\frac{p}{q}\right) = \varphi'\left(\frac{q}{r}\right) \tag{35}$$

where $\langle r\rangle = 1$ for $r = 1$ and $= 0$ for $r > 1$. For the case $\varepsilon = -1$ we find, similarly,

$$\varphi\left(\frac{p}{q}\right) = -\left[\frac{q}{2r}\right] - \varphi\left(\frac{q}{r}\right),$$

$$\varphi'\left(\frac{p}{q}\right) = -\varphi'\left(\frac{q}{r}\right), \quad \varphi''\left(\frac{p}{q}\right) = -\left[\frac{q}{2r} + \frac{1}{2}\right] + \langle r\rangle - \varphi''\left(\frac{q}{r}\right). \tag{36}$$

If p, p_1 are odd relatively prime numbers, and $p > p_1 > 1$ then by successive division, we obtain a series of equalities

$$p_i = k_{i+1} p_{i+1} + \varepsilon_{i+1} p_{i+2}, \qquad i = 0, 1, \ldots, \nu - 1, \; p_{\nu+1} = 1 \tag{37}$$

where $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_\nu$ are equal to ± 1; $p, p_1, \ldots, p_{\nu+1}$ are decreasing odd numbers and $k_1, k_2, \ldots, k_\nu$ are even numbers greater or equal to 2. Equalities (37) give the development of p/p_1 into a continued fraction of the form

$$\frac{p}{p_1} = k_1 + \cfrac{\varepsilon_1}{k_2 + \cfrac{\varepsilon_2}{k_3 + \ddots + \cfrac{\varepsilon_{\nu-1}}{k_\nu + \cfrac{\varepsilon_\nu}{p_\nu}}}} \tag{38}$$

Denoting $\psi(p/q)-\varphi'(p/q)-\varphi''(p/q) = U(p/q)$, we find by means of (35) and (36) for this function, according to algorithm (37), a series of relations

$$U\left(\frac{p_i}{p_{i+1}}\right) = \tfrac{1}{2}(\varepsilon_{i+1}\varepsilon_{i+2}-\varepsilon_{i+1})+\varepsilon_{i+1}\langle p_{i+2}\rangle+\varepsilon_{i+1}\,U\left(\frac{p_{i+1}}{p_{i+2}}\right),$$
$$i = 0, 1, \ldots, \nu-1, \quad \varepsilon_{\nu+1} = -1$$

from which, on eliminating $U\left(\frac{p_1}{p_2}\right), \ldots, U\left(\frac{p_\nu}{p_{\nu+1}}\right)$ we obtain

$$U\left(\frac{p}{p_1}\right) = \tfrac{1}{2}(\varepsilon_1\varepsilon_2\ldots\varepsilon_\nu-\varepsilon_1). \tag{39}$$

Now, let q be an *even* number, let $(p, q) = 1$ and $0 < p < \frac{1}{2}q$ then for functions ψ, ψ', ψ'' defined by (29) after short calculations, we find

$$\psi\left(\frac{p}{q}\right) = \left[\frac{q}{2p}+\frac{1}{2}\right]+\varphi\left(\frac{q-p}{p}\right), \quad \psi'\left(\frac{p}{q}\right) = \varphi'\left(\frac{q-p}{p}\right),$$
$$\psi''\left(\frac{p}{q}\right) = \left[\frac{q}{2p}\right]-\langle p\rangle+\varphi''\left(\frac{q-p}{p}\right),$$

so that

$$\psi\left(\frac{p}{q}\right)-\psi'\left(\frac{p}{q}\right)-\psi''\left(\frac{p}{q}\right) = \left[\frac{q}{2p}+\frac{1}{2}\right]-\left[\frac{q}{2p}\right]+\langle p\rangle+U\left(\frac{q-p}{p}\right).$$

If $p = 1$ then the right hand side of the latter equality also equals to one. If $p > 1$, then for formula (39) to be applicable, we develop $(q-p)/p$ into continued fraction (38); in this development to q/p corresponds a continued fraction of the form

$$\frac{q}{p} = k_1+\cfrac{\varepsilon_1}{k_2+\ddots+\cfrac{\varepsilon_\nu}{k_{\nu+1}}} \tag{41}$$

in which $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_\nu$ are equal to ± 1, the numbers $k_1, k_{\nu+1}$ are *odd*, greater or equal to 3, and $k_2, \ldots, k_\nu$ are *even* numbers greater or equal to 2. Now, applying (39) we find from (40)

$$\psi\left(\frac{p}{q}\right) - \psi'\left(\frac{p}{q}\right) - \psi''\left(\frac{p}{q}\right) + \tfrac{1}{2}(1+\varepsilon_1\varepsilon_2 \ldots \varepsilon_\nu). \tag{42}$$

Thus, between the functions ψ, ψ', ψ'' there exists the following relation: expression $\psi-\psi'-\psi''$ is always equal either to zero or one. To obtain a criterion which does not contain implicitly the elements of the continued fraction (41) and which enables us to determine when this expression is equal to zero and when to one, consider the last but one convergent to fraction (41):

$$\frac{Q}{P_1} = k_1 + \cfrac{\varepsilon_1}{k_2 + \cfrac{\ddots}{\ddots + \cfrac{\varepsilon_{\nu-1}}{k_\nu}}}$$

Using the known recurrence relations between the numerators and denominators of convergents to Q/P, it is easy to establish the following facts: 1) the numerators of convergents are positive increasing from which (since $k_{\nu+1} \geqq 3$) it follows that $q > 2Q$; 2) denominators of two neighbouring convergents are of different parity, from which $P \equiv \nu \pmod 2$. Taking into account equality $pQ-qP = (-1)^\nu \varepsilon_1 \varepsilon_2 \ldots \varepsilon_\nu$ we may write

$$pQ \equiv (-1)^\nu \varepsilon_1 \varepsilon_2 \ldots \varepsilon_\nu \pmod q.$$

this congruence together with the condition $0 < Q < \frac{1}{2}q$ completely determines number Q. Combining this with (42) we may formulate the following proposition: *if the argument r of functions ψ, ψ', ψ'' defined by formula* (29), *is equal to an irreducible fraction p/q lying between* 0 *and* $\frac{1}{2}$, *with even denominator $q > 2$, then these functions are related with one another in such a way that expression $\psi-\psi'-\psi''$ is either equal to zero or one; namely*

$$\psi\left(\frac{p}{q}\right) - \psi'\left(\frac{p}{q}\right) - \psi''\left(\frac{p}{q}\right) = \frac{1+\varepsilon_p}{2},$$

where $\varepsilon_p = \varepsilon(-1)^{(pp'-\varepsilon)/q}$, *where the number p within* 0, $\frac{1}{2}q$ *and unity* $\varepsilon = \pm 1$, *are completely determined by congruence* $pp' \equiv \varepsilon \pmod q$. In particular, for $q \equiv 2 \pmod 4$ and $q \equiv 4 \pmod 8$, the unity has, clearly, the following values:

$$\varepsilon_p = \left(\frac{-1}{pp'}\right) \quad \text{and} \quad \varepsilon_p = \left(\frac{-2}{pp'}\right).$$

Let us now return to formula (32). Applying the latter lemma, we obtain from this formula $h = \sum'(-m/a)$ where sum $\sum'$ is taken over all a within 0, m, relatively prime to $2m$, for which $\varepsilon_a = +1$. The unity $\varepsilon_a = \pm 1$ is determined as follows: on finding for every a a number a' within $0, m$ satisfying congruence $aa' \equiv \pm 1 \pmod{2m}$, we take $\varepsilon_a = (-1/aa')$ for $m \equiv 1 \pmod 4$ and $\varepsilon_a = (-2/aa')$ for $m \equiv 2 \pmod 4$. If $\varepsilon_a = -1$ for some a, then for a' corresponding to it we also have $\varepsilon_{a'} = -1$. From the reciprocity law and the condition $\varepsilon_a = -1$ it is easy to deduce that for such pair of numbers a, a' we always have $(-m/a)+(-m/a') = 0$ so that the sum $\sum''(-m/a)$ taken over all a for which $\varepsilon_a = -1$ is equal to zero. Combining this with the above expression for h, we obtain $h = \sum(-m/a)$ where the summation is performed over all a within 0, m which are relatively prime to $2m$, i.e. the Dirichlet formula (20).

Notes to chapter 6

§ 1. The list of *all* results obtained up until 1922 concerning the number of classes may be found in volume III of Dickson's book [12].

Interesting properties are possessed by the so-called *one-class* determinants, i.e. those numbers $d \equiv 3 \pmod 4$ for which in an improperly primitive positive order of determinant $-d$ there exists only one class of forms; all known numbers of this kind are in the first two rows of the table given in the text:

$$d = 3, 7, 11, 19, 43, 67, 163.$$

According to Gauss's calculations (see the text), checked by Frobenius, there are no more such numbers up to 10000; it is still not known whether they exist beyond this limit. One-class determinants* $-d$ have, for example, the following property: (see Frobenius [18]):

* Heegner Math. Zeitschr. 56, 227–253 (1952) proved that the 9 known determinants are the only possible. See also Stark, Michigan Math. Journal, 1966 Baker, Mathematika, 13 204–216, Ziegel, Acta Arithmetica 1, 83–86 (1935) Deuring, Math. Zeitschrift 37, 405–541 (1933).

if f is a positive, not properly primitive form of determinant $-d = 1-4p$ then every number properly representable by a form $\frac{1}{2}f$ and less than p^2 is a prime. Applying this to the greatest d $(= 163)$, we find that a quadratic polynomial x^2+x+41 gives for the first forty values $x = 0, 1, \ldots, 39$ the following primes:

41, 43, 47, 53, 61, 71, 83, 97, 113, 131, 151, 173, 197, 223, 251, 281, 313, 347, 383, 421, 461, 503, 547, 593, 641, 691, 743, 853, 911, 971, 1033, 1097, 1163, 1231, 1301, 1373, 1447, 1523, 1601.

This fact has already been noted by Euler (see [17], vol. I, p. 584). In the cited paper Frobenius [18] also gives examples of indefinite quadratic forms.

§ **2.** As it was stated in the text, after publication by Kronecker of his relation between the numbers of classes, the other authors obtained many various relations of the same type. We give here the most interesting ones (J. Uspensky [64]):

$$2\sum_{h=0,\,\pm1,\,\pm2,\ldots} F(n-2h^2) = 2\sum_{n=d\delta,\,\delta\text{ odd}}\left(\frac{2}{\delta}\right)d - \sum_{\substack{n=x^2-2y^2\\ x\pm2y>0}} x - 2\sum_{n=2s^2,\,s>0}\{s\}$$

(Stieltjes)

$$2\sum(-1)^h F(n-2h^2) = (-1)^{\frac{1}{2}(n-1)(n-2)}\sum_{n=x^2-2y^2,\,x\pm2y>0} x + 2(-1)^{\frac{1}{2}(n-1)(n-2)}\sum_{n=2s^2,\,s>0}\{s\}.$$

(Stieltjes)

In these relations (and in the subsequent ones) n denotes a given integer and the summation in the left hand side is performed over all integers $h = 0, \pm1, \pm2, \ldots$ for which the argument of function F or G remains greater or equal to zero. It is characteristic that these expressions contain a special numerical function $\sum x$ where the summation is performed over all representations of n by an *indefinite* form x^2-2y^2 with conditions $x+2y>0$, $x-2y>0$.

$$4\sum_{i=1,\,3,\,5,\ldots}(-1)^{\frac{1}{8}(i^2-1)}F\left(\frac{n-i^2}{2}\right) = \sum_{n=s^2+2t^2,\,s>0}(-1)^{\frac{1}{2}(s-1)+\frac{1}{8}(s^2-1)}$$

$s,\ n \equiv 3 \pmod 8$ (Hurwitz),

$$2\sum(-1)^h F(n-3h^2) = \sum_{2n=x^2-3y^2,\, x\pm 3y>0}(-1)^{\frac{1}{2}(x+y)}y + \sum_{4n=i^2+3j^2,\, i,\, j \text{ odd}>0}(-1)^{\frac{1}{2}(j-1)}j + \{s\}_{n=3s^2,\, s>0} \quad n \text{ odd} \quad \text{(Petz)},$$

$$\sum(-1)^h F(4n-5h^2) = \sum_{4n\equiv 5x^2-y^2,\, x+y\equiv 2 \pmod 4,\, 5x>3y>0} y \qquad n \text{ odd (Venkov)},$$

$$\sum_{i=1,3,5,\ldots}(-1)^{\frac{1}{2}(i-1)} iF(8n-i^2) = \sum_{2n=dd',\, d<d',\, d+d' \text{ odd}}(-1)^{\frac{1}{2}(d+d'+1)}d^2 \qquad \text{(Nazimov)}$$

$$8\sum_{h=1,2,3,\ldots} h^2 G(n-h^2) = \frac{Nn}{24} + (-1)^n \sum_{n=dd',\, d<d'}(-1)^{d'}(d'-d)(d'+d)^2 - (-1)^n \sum_{n=d\delta}(-1)^d d^3 \qquad \text{(Humbert)}.$$

In the latter relation N denotes the number of representations of N as a sum of four squares.

§ 3. A vast number of various transformations related to Dirichlet's formulae for positive as well as negative determinant, is given in a detailed memoir of Lerch 'Essais sur le calcul du nombre des classes de formes quadratiques binaires aux coefficients entiers' [46], which won a prize of the Paris Academy of Sciences.* In the memoir 'De nexu inter multitudinem classium etc.' cited in the text, Gauss (see [20], p. 655) gives formulae showing the distribution of quadratic residues of an odd prime modulo in eighths and twelfth parts of the interval $(\frac{1}{8}(r-1)p, \frac{1}{8}rp)$. Denoting by (n) the number of quadratic residues in the interval $(r = 1, 2, \ldots, 8)$ and by $h(-d)$ the number of classes of positive primitive forms of determinant $-d$, we have

1) $p = 8n+1$, $(1) = (8) = \frac{1}{8}[4n+h(-p)+h(-2p)]$, $(2) = (4) = (5) = (7) = \frac{1}{8}[4n+h(-p)-h(-2p)]$, $(3) = (6) = \frac{1}{8}[4n-3h(-p)+h(-2p)]$,

* See L. J. Mordell On Lerch's class number for ordinary quadratic forms.

2) $p = 8n+5$, $(1) = (3) = (6) = (8) = \frac{1}{8}[4n-h(-p)+h(-2p)]$ $(2) = (7) = \frac{1}{8}(4n+3h(-p)-h(-2p)+4]$, $(4) = (5) = \frac{1}{8}[4n-h(-p)$ $-h(-2p)+4]$,

3) $p = 8n+3$, $(1) = (4) = (7) = \frac{1}{8}[4n+2h(-p)+h(-2p)]$, $(2) = (5) = (8) = \frac{1}{8}(4n-2h(-p)+h(-2p)]$, $(3) = \frac{1}{8}[4n+2h(-p)$ $+h(-2p)+4]$, $(6) = \frac{1}{8}[4n-2h(-p)-h(-2p)+4]$,

4) $p = 8n+7$, $(1) = \frac{1}{8}[4n+4h(-p)-h(-2p)]$; $(2) = (3) = (5)$ $= \frac{1}{8}[4n+h(-2p)+4]$, $(4) = (6) = (7) = \frac{1}{8}[4n-h(-2p)+4]$, $(8) = \frac{1}{8}[4n-4h(-p)+h(2p)]$.

Similarly the numbers of quadratic residues of twelfth parts of interval $(0, p)$ are expressed in terms of $h(-p)$ and $h(-3p)$ Gauss's formulae can be easily demonstrated by means of the Dirichlet formulae (20) and (21).

Footnote to page 37.

* It is known that $\varepsilon_n \geqq 4/D_n^{1/n}$ for $0 \leqq n \leqq 24$, where D_0-D_{12} are 1, 4, 12, 32, 64, 128, 192, 256, 256, 512, 768, 972, 729 and $D_{24-n} = D_n$, and this lower bound disproves Hermite's conjecture for $4 \leqq n \leqq 24$. Conway and Leech conjecture that the lower bound is exact for $n \leqq 24$. Blichfeldt proves it exact for $0 \leqq n \leqq 8$, but Chaundy's proofs for $n = 9$, 10 are incomplete. For references see J. W. S. Cassels "An introduction to the geometry of numbers", Springer-Verlag 1959, p. 332, and Leech, Can. J. Math. (1964), 16, 657–682, ibid. (1967) 19, 251–267.

A *very* recent result (Assmus-Matson-Pless-Leech-Conway-Thompson) is that $\varepsilon_{48} \geqslant \sqrt{24}$.

Bibliography

[1] Albert, A. Adrian, The integers represented by sets of ternary quadratic forms, *Amer. J. Math.* 55, (1933) 274–292.

[2] Bachmann, P., *Die Elemente der Zahlentheorie*, Leipzig, 1892, 264 pp. (Part I of 'Zahlentheorie').

[3] Bachmann, P., *Die Arithmetik der quadratischen Formen*, Leipzig, 1898, 668 pp. (Part IV of 'Zahlentheorie')

[4] Bachmann, P., *Niedere Zahlentheorie*, I, und II. Teil, Leipzig, 1902, 1910. 402 pp. and 480 pp. (Bibliography).

[5] Bianchi, L., *Lezioni sulla teoria arithmetica delle forme quadratiche binarie e ternarie*, Pisa 1911–1912, 701 pp. (Litographed).

[6] Borel, E. and Drach, J., *Introduction a l'étude de la théorie des nombres et de l'algèbre superieure*, Paris 1895, 350 pp.

[7] Busche, E., Arithmetischer Beweis des Reciprozitätsgesetzes für die biquadratischen Reste, *J. rein. angew. Math.* 99: 4 (1886) 261–274.

[8] Busche, E. Über die Theorie der biquadratischen Reste, J. *rein. angew. Math.* 141: 2 (1912) 146–161.

[9] Cahen, E., *Theorie des nombres*, t.I, Paris 1914, 408 pp.

[10] Davenport, H., On the distribution of q-th power residues (mod p) *J. London Math. Soc* 7, (1932) 117–121.

[11] Davenport, H., On the distribution of quadratic residues (mod p) II, *J. London Math. Soc.* 8, (1933) 46–52.

[12] Dickson, L. E., *History of the theory of numbers*, vol. III (Quadratic and higher forms), Washington, March 1923, 313 pp. (Bibliography).

[13] Dirichlet, P. G. Lejeune, *Werke*, herausgegeben von L. Kronecker, I. und II. Bd. Berlin 1889 and 1897, 644 pp. and 422 pp.

[14] Dirichlet, P. G. L., *Vorlesungen über Zahlentheorie*, herausgegeben von R. Dedekind, IV, Aufl., Braunschweig, 1894, 657 pp. In 1936 the Russian translation appeared.

[15] Dirichlet, P. G., Lejeune, *Theory of numbers*, St. Petersburg, 1899, 186 pp. (Russian translation of the first three parts of the previous work).

[16] *Encyclopädie der mathematischen Wissenschaften mit Einschluss ihrer Anwendungen*, Band I, Teil II (Zahlentheorie), Leipzig, 1900–1904, pp. 555–1197 (Bibliography).

[17] Euler, L., *Commentationes arithmeticae collectae*, T. I et II, Petropoli, 1849, LXXXVII+584 pp. and 651 pp.

[18] Frobenius G., Über quadratische Formen die viele Primzahlen darstellen, *Sitzungsberichte der Preussischen Akademie der Wissenschaften*, 2 Halbb. (1912), 969–980.

[19] Gauss, C. F., *Werke*, herausgegeben von der Königlichen Gesellschaft der Wissenschaften zu Göttingen, B.II, Göttingen, 1863, 504 pp.

[20] Gauss, C. F., *Untersuchungen über höhere Arithmetik*, deutsch herausgegeben von H. Maser, Berlin 1889, 695 pp. (German translation of 'Disquisitiones arithmeticae and of other Gauss's works in the theory of numbers).

[21] Grave, D. A., *Arithmetical theory of algebraic quantities*, vol. I (Quadratic domain), Kiev, 1910, 372 pp. (litography). (Russian).
[22] Grave, D. A., *Elementary course of the theory of numbers*, 2nd. edition, Kiev, 1913, 315+100 pp. In an appendix to this book are the tables of factorisation into prime factors of all numbers up to 107 999, tables of indices up to 200, tables of development of $\sqrt{n}$ into a continued fraction up to $n = 120$, table of Bernoulli numbers up to B_3 etc.) (Russian).
[23] Hermite, Ch., *Oeuvres*, publies sous les auspices de l'Academie des Science par E. Picard, t.I., Paris, 1905, 498 pp.
[24] Hurwitz, A., Über die Entwicklung complexer Grössen in Kettenbrüchen, *Acta Math.* 11, 2 (1888), 187–200.
[25] Hurwitz, A., Über eine besondere Art der Kettenbruch-Entwicklung reeler Grössen, *Acta Math.* 12, 3 and 4 (1889) 367–405.
[26] Hurwitz, A., Über die angenäherte Darstellung der Zahlen durch rationale Brüche, *Math. Ann.* 44, (1894), 417–447.
[27] Hurwitz, A., Über die Reduction der binären quadratischen Formen, *Math. Ann.* 45 (1894) 85–117.
[28] Hurwitz, A., Über die Kettenbrüche, deren Teilnenner arithmetische Reihen bilden, *Vierteljahrschrift der naturforschenden Gesellschaft in Zürich*, 41: 2 (1896), 34–64.
[29] Hurwitz, A., Über lineare Formen mit ganzzahligen Variabeln, *Nachrichten der Königlichen Gesellschaft der Wissenschaften zu Göttingen*, 2 (1897), 1–7.
[30] Jacobi, C. G., *Canon arithmeticus*, Berolini, 1839, 248 pp.
[31] Jacobi, C. G., *Gesammelte Werke*, herausgegeben von K. Weierstrass, B. VI, Berlin, 1891, 433 pp.
[32] Jouravsky, A. M., Cubic reciprocity law, *Journal of Leningrad Physical-Mathematical Society*, 1: 2, (1927) 204–232. (Russian).
[33] Korkine, A. N., The distribution of integers to a prime modulus and on binomals congruences; with table of primitive roots and characters corresponding to primes, 4000, *Mat. Sbornik* 27: 1 (1909) 28–137. (Russian).
[34] Krečmar, V. A., On divisibility properties of one additive function, *Izvestia Akad. Nauk SSSR* 6: 6 (1933) 763–800. (Russian).
[35] Kronecker, L., *Über bilineare Formen mit vier Variablen*, Berlin, 1884, 60 pp.
[36] Kronecker, L., *Vorlesungen über Zahlentheorie*, herausgegeben von K. Hensel, B. I., Leipzig, 1901, 509 pp.
[37] Landau, E., *Handbuch der Lehre von der Verteilung der Primzahlen*, B. I., Leipzig and Berlin, 1909, 564 pp.
[38] Landau, E., *Vorlesungen über Zahlentheorie*, B. I. (Aus elementaren und additiven Zahlentheorie), Leipzig, 1927, 360 pp.
[39] Legendre, A. M., *Essai sur la théorie des nombres*, Paris, 1808, 480+62 pp.
[40] Legendre, A. M. *Zahlentheorie*, deutsch übertragen von H. Maser, B. I. und II, Leipzig, 1886, 442 and 453 pp. (German translation of the preceeding work).
[41] Lehmer, D. H., Note on Mersenne numbers, *Bull. Amer. Math. Soc.* 38, (1932), 383–384.
[42] Lehmer, D. H., A note on Fermat's last theorem, *Bull. Amer. Math. Soc.* 38, (1932) 723–724.
[43] Lehmer, D. H., On Euler's totient function, *Bull. Amer. Math. Soc.* 38 (1932), 745–751.
[44] Lehmer, D. H., Some new factorizations of $2^n \pm 1$, *Bull. Amer. Math. Soc.* 39, (1933) 105–108.
[45] Lehmer, D. H., Factorisation of certain cyclotomic functions, *Annales of Mathematics*, II. ser. 34 (1933) 461–479.

[46] Lerch, M., Essais sur le calcul du nombre des classes de formes quadratiques binaires aux coefficients entiers, *Memoires présentés par divers savants à l'Academie des Sciences de l'Institut de France*, 33 : 2 (1906) 1–244.
[47] Liouville, J., Sur la forme $x^2+y^2+3(z^2+t^2)$, *J. de math. pur. appliq.* II ser. 5 (1860) 147–148.
[48] Liouville, J., Sur les deux formes quadratiques $x^2+y^2+z^2+2t^2$, $x^2+2(y^2+z^2+t^2)$, *J. de math. pur. appliq.* II ser, 6 (1861) 225–226.
[49] Liouville, J., Sur la forme $x^2+8y^2+8z^2+64t^2$, *J. de math. pur. appliq.* II ser. 7 (1862) 246–247.
[50] Liouville, J., Sur la forme $x^2+y^2+z^2+3t^2$, *J. de math. pur. appliq.* II ser. 8 (1863) 105–107.
[51] Liouville, J., Sur la forme $x^2+2(y^2+z^2+t^2+u^2+v^2)$, *J. de math. pur. appliq.* I. ser., 9 (1864) 175–176.
[52] Liouville, J., Sur la forme $x^2+y^2+5z^2+5t^2$, *J. de math. pur. appliq.* II ser. 10 (1865) 1–2.
[53] Lucas, E., *Théorie des nombres*, t. I., Paris, 1891, 520 pp.
[54] Markov, A. A., *On binary quadratic forms of positive determinant*, St. Petersburg, 1880, 762–800. (Russian).
[55] Markov, A. A., On indefinite quadratic forms with four variables, *Izvestia Akad, Nauk SSSR* 16: 3, (1902) 97–108. (Russian).
[56] Markoff, A., Sur les formes quadratiques ternaires indéfinies, *Math. Ann.* 56: 2 (1903) 233–251.
[57] Markov, V. A., *On positive ternary quadratic forms*, St. Petersburg, 1897, 178 pp. (Russian).
[58] Mertens, F., Über die Äquivalenz der reducirten binären quadratischen Formen von positiver Determinante, *Sitzungsberichte der Kaiserlichen Akademie der Wissenschaften in Wien*, 103: 2 (1894) 1–10
[59] Minkowski, H., *Diophantische Approximationen* (eine Einführung in die Zahlentheorie), Leipzig, 1907, 235 pp.
[60] Minkowski, H., *Geometrie der Zahlen*, Leipzig und Berlin, 1910, 256 pp.
[61] Mordell, L. J., On binary quadratic forms expressable as a sum of three linear squares with integer coefficients, *J. rein. angew. Math.* 167 (1932) 12–19.
[62] Mordell, L. J., Minkowski's theorem on homogeneous linear forms, *J. London Math. Soc.* 8 (1933) 179–182.
[63] Ouspensky, J., Note sur le nombre des représentations des nombres par une somme d'un nombre pair de carrés, *Izvestia Akad. Nauk SSSR VI ser.* 19: 15 (1925) 647–662.
[64] Ouspensky, J., Sur les rélations entre les nombres des classes des formes quadratiques binaires et positives (5 mémoires), *Izvestia Akad. Nauk* VI ser. Premier Mém. I, 19: 12–15 (1925) 599–620; Premier Mém, II 19: 16–17 (1925) 763–784; Deuxième Mém. I.20: 1–2 (1926) 25–38; Deuxième Mém. 20: 3–4 (1926) 175–196; Troisième Mém, 20: 5–6 (1926) 327–348; Quatrième Mém., 20: 7–8 (1926) 574–566; Cinquième Mem., 20: 9 (1926) 619–642.
[65] Ouspensky, J., On Gierster's Classnumber Relations, *Amer. Journ. Math.* 50: 1 (1928) 93–122.
[66] Ouspensky, J., On the number of representations of integers by certain ternary quadratic forms, *Amer. Journ. Math.* 51: 1 (1929) 51–60.
[67] Pall, G., The structure of the number of representations function in a positive binary quadratitc form, *Math. Z.* 36 (1933) 321–343.
[68] Pall, G., The structure of the number of representations function in a binary quadratic form, *Transactions American Math. Soc.*, 35 (1933) 491–509.

[69] Perron, O., *Die Lehre von den Kettenbrüchen, Leipzig und Berlin* 1913, 520 pp. (Bibliography).
[70] Posse, K. A., Table of primitive roots and corresponding characters for primes between 4000 and 5000, *Mat. Sb.* 27: 2 (1909) 175–179. (Russian).
[71] Posse, K. A., Table of primitive roots and corresponding characters for primes between 5000 and 10 000, *Mat, Sb,* 27 : 2 (1909) 238–257. (Russian).
[72] Ramanujan, S., *Collected papers,* edited by G. H. Hardy, P. V. Sechu Aiyar and B. M. Wilson, Cambridge, 1927, 355 pp.
[73] Redei, L. Arithmetischer Beweis des Satzes über die Anzahl der durch vier teilbaren Invarianten der absoluten Klassengruppe in quadratischen Zahlkörper, *J. rein angew. Math.* 171: 1 (1934) 55–60.
[74) Reichardt, H., Zur Struktur der absoluten Idealklassengruppe im quadratischen Zahlköper, *J. rein angew. Math.* 170 (1933) 75–82.
[75] Ross, Arnold E., On representation of integers by indefinite ternary quadratic forms of quadratfrei determinant, *Amer. J. Math.* 55 (1933) 293–302.
[76] Smith, H. J. St., Note on continued fractions, *Messenger of Mathematics,* II ser, 6 (1876) 1–14.
[77] Schrödei, J., Zur Darstellung der Moebiusschen Function durch grösste Ganze, *Mitteilungen der mathematischen Gesellschaft in Hamburg* 7 (1932) 89–93.
[78] Schur, I., Über die Existenz unendlich vieler Primzahlen in einigen speziellen arithmetischen Progressionen, *Sitzungsberichte der Berliner Mathematischen Gesellschaft,* 11: 3 (1921) 40–50.
[79] Serret, J. A., *Cours d'algèbre supérieure,* t.I, 4 ed., Paris, 1877, 647 pp.
[80] Stieltjes, T. J., *Oeuvres complètes,* publiées par les soins de la Société Mathématique d'Amsterdam, t.I et II, Groningen, 1914 and 1918, 471 pp and 603 pp.
[81] Chebychev, P. L., *Collected works,* edited by A. A. Markov and H. J. Sonin, vol. I, Petersbourgh, 1899, 714 pp. (Russian).
[82] Chebychev, P. L., *Theory of congruences,* 2nd ed., Petersbourgh, 1879, 223 pp. (Russian).
[83] Vahlen, K. Th., Beiträge zu einer additiven Zahlentheorie, *J. rein. angew. Math.* 112, (1893).
[84] Vahlen, K. Th., Über Näherungswerthe und Kettenbrüche, *J. rein. angew. Math.* 115 : 3 (1895) 221–233.
[85] Vassiliev, A. V., *The Integer,* Petersbourgh, 1919, 268 pp. (Russian).
[86] Vinogradoff, I., Sur la distribution des résidus et des non-résidus des puissances, *Journal of Physical Math. Soc. of Perm University* 1: 1 (1918) 94–98.
[87] Vinogradov, I. M., Elementary proof of one general theorem of analytic theory of numbers, *Izvestia Akad. Nauk SSSR VI,* ser. 19 (1925) 785–796. (Russian).
[88] Vinogradov, I. M., On the distribution of indices, *Doklady Akad. Nauk SSSR* 2 (1926) 73–76. (Russian).
[89] Vinogradov, I. M., Some theorems on the distribution of indices and primitive roots, *Trudy Phys. - Math. Inst. Steklov,* 5 (1933) 87–93. (Russian).
[90] Vinogradov, I. M., New applications of trigonometrical sums, *Doklady Akad Nauk SSSR* 2: 1 (1934) 1–5. (Russian).
[91] Vinogradov, I. M., A new solution of Waring problem, *Dokl. Akad. Nauk SSSR,* 2: 6 (1934) 337–341. (Russian).
[92] Vinogradov, I. M., New theorems on distribution of primitive roots, *Dokl. Akad. Nauk SSSR* 2: 7 (1934) 1–4. (Russian).
[93] Weber, H., *Lehrbuch der Algebra,* B.II, 2. Aufl., Braunschweig, 1899, 855 pp.
[94] Weber, H. and Wellstein, J., *Encyclopedia of elementary mathematics,* vol. I. (algebra and analysis), 2nd ed., Odessa, 1911, 666 pp. (Published by Mathesis). (Russian).

[95] Venkov, B. A., On arithmetic of quaternions, (5 communications) *Izvestia Akad. Nauk SSSR* VI ser. I communication, 16 (1922) 205-220; II communication 16 (1922) 221–246; III communication *Izvestia Akad. Nauk SSSR* VII ser. 2: 5 (1929) 489–504; IV communication 2: 6 (1929) 607–622. (Russian).

[96] Venkov, B. A., Über die Klassenzahl positiver binarer quadratischer Formen, *Math. Z.*, 33: 3 (1931) 350–374.

[97] Western, A. E., On Lucas's and Pepin's tests for primeness of Mersenne's numbers, *J. London Math. Soc.*, 7 (1932) 130–137.

[98] Zolotarev, E. I., *Complete works*, edited by Physical-Mathematical Steklov Institute of Acad. Sci SSSR, I, Vol. Leningrad, 1931, 434 pp. II vol. Leningrad, 1932, 364 pp.

The following books may also be recommended:

H. Davenport: The higher Arithmetic Hutchison's University Press London, 1952.

Hardy and Wright: An introduction to the theory of Numbers. Clarendon Press, Oxford, 1965.

J. Nagell: Introduction to number theory. Almqvist and Wiksell Stockholm.

Uspensky and Haslet: Elementary Number Theory McGraw Hill Book Company 1939.

Vinogradov: Introduction to the Theory of Numbers Pergamon Press 1955.

Khinchin: Three pearls of number theory, Graylock Press, Rochester N.Y. 1952.

Index

Abelian group 132
adjoint forms 148, 153
ambiguous class 121, 173
ambiguous forms 121, 122
amicable numbers 27
arithmetical functions 177
associated forms 122
associated numbers 95

Bernoulli, Johann 65
Bernoulli numbers 12
Bernoulli sequence 67
biquadratic residues 82
binary quadratic form 99
Borel theorem 43

chain of forms 38
character 140
charactecistic number 154
class number 104, 133, 215, 216
complete quotient 41, 64
complete system of residues 6
composition 127
compounded 132, 162
concordant 130, 145
continued fraction 1, 39
convergent 40
cubic residues 89

Davenport 214
Diophantine approximations 32
Dirichlet formulae 228
Dirichlet theorem 33
double modulus 20
double partitions 183

Eisenstein rule 31
Euclidean Algorithm 1, 24
Euler theorem 6
Euler criterion 16
Euler-Legendre theorem 178, 180
equivalent numbers 44
equivalent quadratic forms 38

Fibonacci series 69
Farey series 32
Fermat 27, 165
Fermat quatioent 28
Fermat theorem 6, 9
figurate numbers 165

Gauss first proof of quadratic reciprocity law 72
Gauss's formula 216
generic characters 140, 173
genus 141

Hermite theorem 37

idoneal numbers 71, 218
improperly primitive forms
  quadratic 118
  ternary 148
indefinite forms 37, 121, 173
index 10
invariants of Abelian group 133
inversion formula 3
inverse numbers 61

Jacoby symbol 19

Kronecker theorem 34

Lagrange 8, 47
Lagrange theorem 60, 8
Least primitive root 29
Legendre criterion 42
Legendre symbol 15
Lehmer 25
Liouville's identities 190
Lucas 25

Mersenne numbers 25
Minkowski theorem 35

Möbius function 3

neighbouring forms 38, 107
number of representations
x^2+y^2 52
x^2+2y^2 53
x^2+3y^2 54
x^2-2y^2 56
} 200
number of representations by three squares 165

opposite forms 121

parallel forms 125
partitions 176
Pellian equation 50, 62, 103, 113
pentagonal number 174
perfect number 3
period of continued fraction 60, 71
period of forms 108, 109, 111
point graphs 176
positive forms 37
primary numbers 96
primitive root 9
principal form 119
principal genus 141
properly primitive forms
quadratic 118, 139
ternary 148
proper representation 99, 153
purely periodic continued fraction 60

quadratic residue 14
quadratic irrationality 58
quadratic reciprocity 16, 72
quotient 40

Ramanujan theorem 187
Redéi theorem 164
reduced forms 39, 104, 106, 115
reduced number 59
reduced system of residues 6
regular determinant 217
relative minimum 47
representation by three squares 164
residue of degree n 11

Serret theorem 44
simplest form 119
Smith's theorem 213
subgroup G 142
symmetric continued fractions 56

ternary forms 146
triangular numbers 174

Vahlen theorem 43, 212
Vinogradov 29, 214

Waring problem 213
Wilson theorem 8

A. O. Gelfond

THE SOLUTION OF EQUATIONS IN INTEGERS

Translated from the 2nd Russian edition by Leo L. Boron

A popular discussion of various methods of solving problems in the area of finding integer solutions of equations. Theorems, formulated in this booklet, are provided with proofs in those cases where these proofs are sufficiently simple.

A. Ya. Khintchine

CONTINUED FRACTIONS

Translated by Peter Wynn

This is a translation of the third and latest edition of the monograph. It deals with the properties of the so-called simplest continued fraction

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \dots}}$$

and the uses to which this can be put in the investigations of the aritmetic properties of continuum, in particular of the laws governing the approximation of algebraic and transcendental numbers by means of rational numbers.

J. L. Koksma and L. Kuipers

ASYMPTOTIC DISTRIBUTION MODULO ONE

This work contains the lectures given at the colloquium on Asymptotic Distribution Modulo One which was held in Breukelen (The Netherlands) under the auspices of N.U.F.F.I.C.

I. P. Mysovskih

LECTURES ON NUMERICAL ANALYSIS

Translated by L. B. Rall

The aim of this book is to develop its topics in a manner which is mathematically rigorous, but easy to follow. A number of numerical examples are given to assist the reader. The book is suitable for home-study or as a textbook for an introductory course in numerical analysis for students of applied mathematics, computer sciences, engineering, or physical sciences.

WOLTERS-NOORDHOFF PUBLISHING